

Lecture Notes in Computer Science

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

2770

Springer

Berlin

Heidelberg

New York

Hong Kong

London

Milan

Paris

Tokyo

Eberhard Becker Willms Buhse
Dirk Günnewig Niels Rump (Eds.)

Digital Rights Management

Technological, Economic,
Legal and Political Aspects



Springer

Editors

Eberhard Becker
Universität Dortmund, Fachbereich Mathematik
44221 Dortmund, Germany
E-mail: becker@digital-rights-management.org

Willms Buhse
Elbchaussee 13, 22765 Hamburg, Germany
E-mail: buhse@digital-rights-management.org

Dirk Günnewig
Niederste Kirchhof 8, 59510 Lippetal, Germany
E-mail: guennewig@digital-rights-management.org

Niels Rump
16 Chatsworth Avenue, Bromley, Kent, BR1 5DP, Great Britain
E-mail: rump@digital-rights-management.org

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie;
detailed bibliographic data is available in the Internet at <<http://dnb.ddb.de>>.

CR Subject Classification (1998): E.3, C.2.0, D.2.11, D.4.6, H.2.0, H.3, H.4, H.5.1,
K.4.1, K.4.4, K.6.5

ISSN 0302-9743

ISBN 3-540-40465-1 Springer-Verlag Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag is a part of Springer Science+Business Media
springeronline.com

© Springer-Verlag Berlin Heidelberg 2003
Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Protago-TeX-Production GmbH
Printed on acid-free paper SPIN: 10941270 06/3142 5 4 3 2 1 0

Preface

Digital Rights Management (DRM) is a topic of interest to a wide range of people from various backgrounds: engineers and technicians, legal academics and lawyers, economists and business practitioners. The two conferences on the issue held in 2000 and 2002 in Berlin, Germany, brought these people together for fruitful discussions. This book continues this process by providing insights into the three main areas that DRM influences and that DRM is influenced by: technology, economics, and law and politics.

Looking at the first results of the two conferences we would like to emphasize three aspects. Firstly, DRM is a fairly young topic with many issues still unresolved. Secondly, there is still an acute lack of objective information about DRM and the consequences of using (or not using) DRM in our Information Society. And, finally, only open discussions amongst all the interested parties and people from different scientific and practical backgrounds can help to create a foundation on which DRM can actually become useful.

We have tried to provide some of this missing information by inviting high-profile authors from various backgrounds. Thus, this book provides the first interdisciplinary overview of DRM. We hope that the reader will find sufficient food for thought, which will hopefully lead to a more holistic view and a wider discussion on how to manage and protect intellectual property in the “Digital Age.”

A book like this needs many people to lend a hand. We would like to express our appreciation to the Ministry of Research of North Rhine-Westphalia — especially Dr. Michael Schmidt and Dr. Erich Köster — for their generous funding of the Research Alliance Data Security, North Rhine-Westphalia, the two conferences, and this study.

We would also like to thank the European Institute for IT Security at the University of Bochum (EUROBITS) — especially Petra Henseler, Marcus Heitmann, Prof. Dr. Christof Paar, Ulrike Schneider-Schlepppe and Hellen Tackenberg.

The two conferences were organized by the Research Alliance Data Security, North Rhine-Westphalia (subprojects at the Universities of Bochum and Dortmund), and coorganized by and held at the German Federal Ministry for Economics and Technology (Ministry of Economics and Labour) and the Association of German Chambers of Industry and Commerce (DIHK), respectively. We would like to thank the BMWi and DIHK — especially, Dr. Ulrich Sandl, Hubertus Soquat, Dr. Ina Pernice, Claudia Lorenz and Dana Lange — the participants and, of course, the speakers for their insightful talks.

Such a broad and interdisciplinary overview cannot be realized without the input of the many excellent authors who contributed to this book. We wish to express our deep gratitude to them. Special thanks go to Michael Abshoff and Dietmar Paltner, and especially to Stefan Kühling (our \LaTeX wizard), at the University of Dortmund.

We hope that this book helps you to understand what DRM is, how it can be used, and in what contexts DRM systems and components will “live.”

That said, all authors and interested readers are welcome to continue to share new or update existing articles and their views at

www.digital-rights-management.org

or e-mail the editors for any comments — positive or negative — at

editors@digital-rights-management.org

September 2003

Eberhard Becker, Willms Buhse,
Dirk Günnewig, Niels Rump



<http://www.digital-rights-management.org>

Funded by



Ministry of
Science and Research
North-Rhine Westphalia

<http://www.bildungsportal.nrw.de/BP/Ministerium/>

Supported by

Universität Dortmund



<http://www.uni-dortmund.de>



<http://www.datensicherheit.nrw.de>

Contents

- 1 DRM as an Interlocking Challenge for Different Scientific Disciplines:
Introduction
Eberhard Becker, Willms Buhse, Dirk Günnewig, Niels Rump 1
- 2 Digital Rights Management: Technological Aspects 3
 - 2.1 Definition, Aspects, and Overview
Niels Rump 3
 - 2.2 Requirements for DRM Systems
Richard Gooch. 16
 - 2.3 Components of DRM Systems 26
 - 2.3.1 Identification and Metadata
Norman Paskin 26
 - 2.3.2 Authentication, Identification Techniques, and Secure Containers — Baseline Technologies
Gabriele Spenger 62
 - 2.3.3 Digital Watermarking
Fabien A.P. Petitcolas 81
 - 2.3.4 Content Based Identification (Fingerprinting)
Jürgen Herre 93
 - 2.3.5 Rights Expression Languages
Susanne Guth. 101
 - 2.3.6 Electronic Payment Systems
Ahmad-Reza Sadeghi, Markus Schneider. 113
 - 2.3.7 Mobile DRM
Frank Hartung 138
 - 2.4 A Sample DRM System
Susanne Guth 150
 - 2.5 DRM and Standardization — Can DRM Be Standardized?
Spencer Cheng, Avni Rambhia 162
 - 2.6 Trusted Platforms, DRM, and Beyond
Dirk Kuhlmann, Robert A. Gehring 178
 - 2.7 DRM Under Attack: Weaknesses in Existing Systems
Tobias Hauser, Christian Wenz. 206
 - 2.8 If Piracy Is the Problem, Is DRM the Answer?
Stuart Haber, Bill Horne, Joe Pato, Tomas Sander, Robert Endre Tarjan 224

3	Digital Rights Management: Economic Aspects	234
3.1	The Basic Economic Theory of Copying <i>Tobias Bauckhage</i>	234
3.2	Facing the Music: Value-Driven Electronic Markets, Networks and Value Webs in Economic Integration of Digital Products <i>Rolf T. Wigand</i>	250
3.3	Creating a Framework for Business Models for Digital Content — Mobile Music as Case Study <i>Willms Buhse, Amélie Wetzel</i>	271
3.4	Impacts of DRM on Internet Based Innovation <i>Arnold Picot, Marina Fiedler</i>	288
3.5	Evaluating Consumer Acceptance for Protected Digital Content <i>Marc Fetscherin</i>	301
3.6	Lessons from Content-for-Free Distribution Channels <i>Michel Clement</i>	321
3.7	Standardization in DRM — Trends and Recommendations <i>Oliver Bremer, Willms Buhse</i>	334
3.8	The Darknet and the Future of Content Protection <i>Peter Biddle, Paul England, Marcus Peinado, Bryan Willman</i> . . .	344
4	Digital Rights Management: Legal and Political Aspects	366
4.1	Protection of Digital Content and DRM Technologies in the USA	366
4.1.1	Protection under US Copyright Law <i>Mathias Lejeune</i>	366
4.1.2	The Copyright Wars — A Computer Scientist’s View of Copyright in the U.S. <i>Barbara Simons</i>	383
4.2	Protection of Digital Content and DRM Technologies in the European Union	405
4.2.1	European Copyright — Yesterday, Today, Tomorrow <i>Jörg Reinbothe</i>	405
4.2.2	DRM and Privacy — Legal Aspects in the European Union <i>Lee A. Bygrave</i>	418
4.2.3	Private Copying and Levies for Information- and Communication-Technologies and Storage Media in Europe <i>Constanze Ulmer-Eilfort</i>	447

4.2.4	Tipping the Scale in Favor of the Right Holders: the European Anti-Circumvention Provisions <i>Séverine Dusollier</i>	462
4.3	Protection of Digital Content — Germany	479
4.3.1	The German Copyright — Yesterday, Today, Tomorrow <i>Thomas Dreier, Georg Nolte</i>	479
4.3.2	Copy Protection by DRM in the EU and Germany: Legal Aspects <i>Bettina Goldmann</i>	502
4.3.3	Implementation of the European Info Directive in German Law and Its Consequences for Teaching and Research <i>Bettina Böhm</i>	520
4.3.4	New Copyright for the Digital Age: Political Conflicts in Germany <i>Dirk Günnewig</i>	528
4.4	Copyright Dilemma: Access Right as a Postmodern Symbol of Copyright Deconstruction? <i>Thomas Hoeren</i>	574
4.5	Business, Technology, and Law — Interrelations of Three Scientific Perspectives on DRM <i>Johannes Ulbricht</i>	587
4.6	The Present and Future of DRM — Musings on Emerging Legal Problems <i>Stefan Bechtold</i>	597
A	Getting Insights: DRM Conferences 2000 and 2002 <i>Eberhard Becker, Dirk Günnewig</i>	655
A.1	DRM Workshop 2000: Summary	657
A.2	DRM Conference 2002: Summary	664
B	Authors	685
C	References	701
D	Index	799

1 DRM as an Interlocking Challenge for Different Scientific Disciplines: Introduction

*Eberhard Becker*¹, *Willms Buhse*², *Dirk Günnewig*¹, *Niels Rump*³

There is music on the Internet! — a realization that was news five years ago is common knowledge today. In fact, there is much more music — and indeed other “content” than rights holders and the “content industries” would like to think. It is the special feature of the Internet and digital technologies that copies can be easily produced and distributed to millions of recipients at very low costs. New fast and efficient channels for the distribution of music, of videos, pictures and books, present a unique opportunity to open new markets with expectations of large revenues: a gold-rush in the internet age.

However, gold digging and what some would call robbery come together. Downloading content from the web without paying a single cent or penny to the artist or the distributor is an easy game — and it is played worldwide. Content industries claim the loss of billions of Euros per year. Also, it is feared that creativity and the power of innovation will decline as the opportunity for financial reward becomes severely diminished.

Digital Rights Managements — DRM for short — is one of the weapons that the content industries want to bring into action in this battle. DRM systems associate “rules” to content that are usually used to impose constraints on the use and distribution of digital goods. In this way, so the argument goes, DRM will help to enable new business models that can benefit from the apparently unlimited potential of the Internet. Hence, the return on investment is no longer so endangered and a new world of opportunity for artists, producers as well as consumers can be realised.

At the other extreme, some campaigners, particularly advocates of “fair use”, “free speech” and unrestricted access to information tend to interpret DRM to mean “Digital Restriction Management”. Their view is that the basic rights of users are violated because rights holders are able to use DRM to enforce restrictions on users where previously they were able to exercise fair use exceptions. Moreover, the view is that the rights of content owners will take precedent over the legitimate rights of consumers. Hence, DRM Systems are regarded as a blessing or as an evil, depending on different points of view.

It is not the aim of this book to side with either of these extremes. Rather, it presents a broad spectrum of articles and arguments centred on the use of DRM. The primary goal is to shed light on this highly controversial topic from various relevant viewpoints and scientific disciplines. In order to focus the discussion the book mainly considers the distribution of entertainment content (i.e. as music,

¹ Universität Dortmund.

² Bertelsmann Digital World Services.

³ Rightscom Ltd.

pictures, movies, text, etc). The application of DRM systems inside companies' own intranets, albeit of great interest in its own, is set aside.

It is important to realise that the management of digital rights has to take three very different perspectives into account, namely, technical, legal and business issues. The design of this book mirrors this multidisciplinary characteristic of the topic. In order to understand the scope and the limitation of DRM technology a certain familiarity with the technology is needed and this is provided in the second chapter (just after this introduction). The other (legal and business) issues are dealt with in the subsequent sections. Each of these three main chapters concludes with an interdisciplinary article that provides an insight into future trends.

In recent years, various legislative actions have been taken to provide a legal basis for the relationships between content providers and content users. In 1996, the treaties of the World Intellectual Property Organization (WIPO) were signed, followed by the U.S. Digital Millennium Copyright Act (DMCA) two years later. In Europe, the European Commission issued its European Copyright Directive in 2001 on the basis of which, amongst others, the German Copyright Law was amended in 2003. Hence, the legal discussions in this book focus on the situation within the European Union and, especially, Germany. This is not to say, that similar discussions on the relationship between DRM systems and Intellectual Property are not being held all over the world. However, the cases of the EU and Germany illustrate the fundamental issues and fields of conflict, although this book also looks across the Atlantic, to investigate the lessons learnt from the operation of the US copyright legislation.

Compared to the technical and legal issues, the usage and benefit of DRM systems from a business perspective has been the least explored. There are a number of reasons for this of which two should be highlighted. Firstly, the Internet brought us concepts such as the so-called "attention economy" (sometimes also called "the fight for eyeballs"). The consequence of this was that there was initially little attempt (or from some value chain participants a need) to protect content and generate revenue streams directly from it. The vast majority of early Internet uses of content involved promotional and largely free distribution models with no regard for protection issues. Secondly, the earliest users of the Internet were academics whose natural culture was to share ideas. This peer-to-peer (p2p) culture still remains even though the Internet medium is now widely adopted by businesses as a new source of content revenue. Still there is an inherent conflict between the culture of sharing where protection is of minimal, if any, importance, and the business need to trade content in a protected environment which requires the deployment of DRM technology. The economic chapter therefore focuses on several key topics such as the definition of copying, electronic markets, business models, impacts on innovation and consumer acceptance of DRM systems. Additionally the impact of standardisation and the influence of free distribution channels — sometimes called the "Darknet" — are illustrated.

2 Digital Rights Management: Technological Aspects

2.1 Definition, Aspects, and Overview

*Niels Rump*⁴

Abstract: Digital Rights Management is a fairly recent technology — it came into use only in the mid 1990s. Nevertheless, it has already lived through a life cycle of ups and downs that many technologies would require decades for.

Digital Rights Management, or DRM, has been called “the saviour” of intellectual property rights as well as “completely useless” in protecting assets; it has been said that it is “accepted and is used” by the participants in the content value chain while others say DRM is “not used at all”.⁵

This paper takes a closer look at the role of DRM in distributing content through networks such as the Internet and indicates what types of technology are available, in what environments they exist and how well today’s DRM systems fulfil what is expected of them by various members of the content value chain.

I Introduction

Before embarking on the discussion about “Digital Rights Management”, the term itself needs defining. Unfortunately there are many definitions, depending of the viewpoint of the person providing the definition. One such definition is given in whatis.com⁶:

Definition 1.

“Digital rights management (DRM) is a type of server software developed to enable secure distribution — and perhaps more importantly, to disable illegal distribution — of paid content over the Web. [...]”

While this definition is definitely true, and it represents a fairly dominant view on what DRM is and provides, it does not give the full picture as it omits looking at the environment in which DRM Systems are to be used. Figure 1 shows this environment by providing the steps that most content goes through when being traded⁷: production, digitisation, identification, ascription of descriptions, distribution, use (by a consumer), monitoring of use, and collection of money. Any of these steps may be omitted in certain circumstances. For example, if content is distributed “for free” the step of collecting money will not need to be executed.

Digital Rights Management plays a role in *every step* depicted in the diagram and listed above. Hence, a more generic definition can be given as follows⁸:

⁴ Rightscom Ltd.

⁵ See: *Günnewig* within this book on page 528.

⁶ See: whatis.com (2002).

⁷ The term “trade” includes commercial trade for money using a variety of business models as well as peer-to-peer distribution where usually no money changes hands and other non-revenue generating trades such as “promotion”.

⁸ See: *Iannella* (2001).

Definition 2.

“DRM covers the description, identification, trading, protecting, monitoring and tracking of all forms of usages over both tangible and intangible assets. [...]”

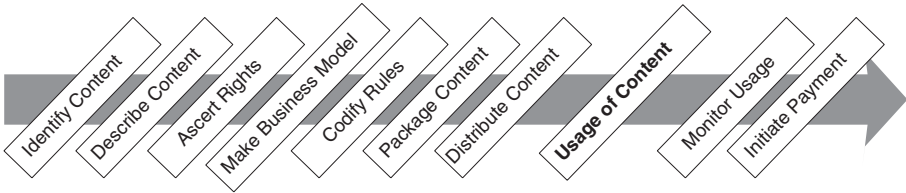


Fig. 1. Different Steps of Trading Content

In short, DRM includes *everything* that someone does with content in order to trade it. These DRM functions can be split into two groups as depicted in Figure 2:



Fig. 2. The two Parts of DRM

Firstly, DRM is about *managing digital rights* (depicted as the “Management” box in Figure 2). Rights holders need to identify their content (how else does a content or rights owner know what right he really owns?), they need to collect metadata⁹ to the content (how else should potential customers of such content be able find what they want to obtain?), they need to assert what rights they have in the content (only when knowing this can he actually attempt to distribute content), and they need to develop business models for distributing their assets¹⁰.

Secondly, DRM is about *digitally managing of rights*, or enforcing exploitation rules as determined by the rights holder (or any of the rights holder’s business partners, such as distributors, wholesalers, e-sellers, etc.). This second group of DRM functions is what Definition 1 speaks about; it is also this definition, with most people have in mind, when discussing DRM. Most of the “DRM technologies” (as briefly introduced in Section III of this article) fall into this second group of DRM functions.

II Environment for DRM Systems

Different elements of DRM systems are used in different stages of content trading as depicted in Figure 1. This already shows that these technical elements are not operating in isolation. In fact, the technologies used are dependent on the business models in operation and these, as well as the technologies themselves, depend on the legal system that prevails. For example, it would be imprudent to use high-security technology to protect content with comparatively low value or to use technology that offers little

⁹ The physical ascription of metadata falls into the second group of DRM functions.

¹⁰ The expression of such permitted forms of exploitation using a “Rights Expression Language” falls, again, into the second group of DRM functions.

protection when the content to be protected is of very high value. Similarly, protecting content with cryptographic technologies that are illegal in key markets will not enable a business to flourish and is bound to fail.

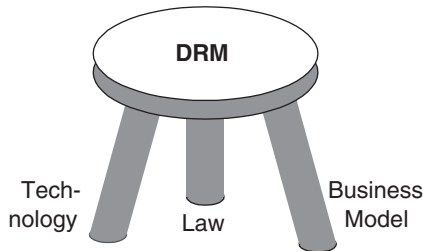


Fig. 3. Three Crucial Elements of DRM — the “three Legged Stool”

The three columns for DRM systems (technology, business models, and the legal underpinnings) can be compared to a three-legged stool which can stand upright only when all three legs are of the same length. As soon as one leg is too short (or, in fact, too long) the stool will fall over. Unfortunately, unlike a three-legged stool which, when all legs are the same length is fairly stable, the same does not apply to DRM systems. They are subject to influences by several external factors and it is those factors, that can lead to DRM systems not being used even when the technology is working properly. These influences, as described in some detail below, ultimately determine the success of DRM.

II.1 Economic Aspects

Economic aspects, such as the market situation, play a major role for rights holders and content distributors in determining which business models for distributing content and which technology (DRM and others) to use for supporting their business models. They of course also determine whether consumers are willing to obtain¹¹ content in new formats through new content delivery services — which usually also means the purchase of new equipment (e.g. an ebook reader, an internet-ready home stereo system or a digital television set).

The uncertain commercial climate following the burst of the “dot.com bubble” was certainly detrimental to the uptake of such content delivery services.

II.2 Social Aspects

The question of how socially acceptable it is to use DRM systems is the second critical issue which influences the promotion and use of DRM-governed content.

Why should a customer start using software with DRM components that, by their nature, limit the customer’s freedom in interacting with the content? Only when the majority of customers can be convinced that DRM is an appropriate mechanism for enjoying content, will they start to regularly use it.¹²

¹¹ Similar to footnote 7 on “trade” above (see page 3), the notion of obtaining content includes buying content for money as well as obtaining it “for free”. See: *Fetscherin* within this book on page 301.

¹² See: *Günnewig* within this book on page 528.

Providing “added value” to such DRM-protected content seems to be a possibility for achieving this goal. Unfortunately for the DRM providers and rights holders in the context of the music industry, the proliferation of unprotected ISO/MPEG Audio Layer III (mp3) content¹³ has already created a mind set that music can be freely copied and shared which puts a further burden on providing added value that has to be offered.¹⁴

Other social aspects also influence the uptake of DRM systems. For example the discussions on the tension between the right to protect ones intellectual property (as laid down in most countries’ copyright laws) and concerns over the erosion of “fair use” issues (as championed by the academic and library communities as well as, increasingly, by pressure groups for the handicapped) have dominated the discussion about DRM Systems. While many DRM systems can technically handle both aspects, their *use* has so far been geared towards the protection, leading to even more resistance to the concept and usage of DRM. Thus the aforementioned discussions can be expected to continue for the foreseeable future.

These objections against the use of DRM with content need to be overcome by an informed and open discussion and a sensible use of technology in sensible business models in order to create a social environment that is accepting of DRM.

II.3 International Aspects

The above issues cannot, however, be examined on a purely national basis and have to be investigated in an international context because for a variety of reasons:

1. The production and dissemination of content is in many cases too expensive for the content to only be disseminated in one territory. Hence, the rights situation in several countries will have to be taken into account.
2. The laws protecting intellectual property are significantly varied from country to country, despite recent efforts towards international harmonisation.
3. And last, but certainly not least, any content made available on the internet, even if intended to be distributed into one country only, is automatically available to internet users all over the world.¹⁵

Only when all these aspects are taken into account, can a working DRM system with all its components become successful, not only in protecting content, but also in supporting content distribution through viable business models.

¹³ One should better say: “technically unprotected mp3 files” as the content in these files is, in most cases and jurisdictions, still *legally* protected.

¹⁴ See: Rump, Herre, Brandenburg, Koller, Allamanche (1999).

¹⁵ Some DRM systems are able to limit the accessibility to the content to certain countries. That, however, requires that the DRM system runs on devices that provide support for that particular DRM system and which operate in these countries. This may lead to problems, in countries where copyrights laws do not sufficiently protect the viability of such systems — or even make them illegal.

III Components of DRM Systems

As described in Section I of this article, DRM Systems have to fulfil a variety of tasks. For each of these a variety of tools exists as described below.¹⁶

1. *Secure containers* make the content inaccessible to those users that are not authorised to access the content. These containers mainly rely on cryptographic algorithms such as DES¹⁷ or AES¹⁸. An early example is the Multimedia Protection Protocol (MMP) developed by Fraunhofer IIS¹⁹. Other examples include SDC's Digital Multimedia Object, InterTrust's DigiBox and DigiFile, and Microsoft's file format for ebooks `.lit`.
2. *Rights expressions* are used to express to whom access to the content wrapped in secure containers is permitted. Such rights expressions are formed either using simple rights expression flags or complex Rights Expression Languages such as ISO/MPEG's Right Expression Language²⁰ in conjunction with its Rights Data Dictionary²¹.

Fraunhofer's MMP is an example of a system using only simple rights expressions (MMP only allows music playback on one authorised machine) while the other examples given above all allow complex rights expressions. To what extent complex expressions will be practical in "small footprint devices" such as mobile phones and PDAs²² remains to be seen.

3. Content *identification and description* systems are used to uniquely identify the content (e.g. International Standard Book number²³) and to associate descriptive metadata with the content (e.g. SMPTE's²⁴ Metadata Dictionary²⁵).

Often content identification systems are combined with content description systems. For example, for each International Standard Work Code (ISWC) a minimal set of metadata (including items such as title, author, composer, etc.) will be created. Similarly, minimal metadata exists for the International Standard Book Number (ISBN) which has been in use for several decades. However no ISBN metadata data is *electronically* available, which forces online booksellers such as Amazon.com to capture their own metadata. This data is, however, of less value than the original data because of data re-entry problems (when data is re-keyed into systems where typos can create serious problems).

Such data — from the original source or not — can then be used, for example, by retailers for their stock control systems. The combination of ISBNs and book-related metadata has become very popular with consumers to, for instance, find, order and buy books.

Such identification systems also exist for other media types (e.g. International Standard Recording Codes (ISRC) for sound recordings, International Standard

¹⁶ A more in-depth discussion of some of these components can be found in subsequent articles within this book.

¹⁷ Data Encryption Standard.

¹⁸ Advanced Encryption Standard, also known as Rijndael.

¹⁹ See: Rump (1996).

²⁰ See: MPEG-21 REL (2003).

²¹ See: MPEG-21 RDD (2003).

²² Personal Digital Assistants.

²³ See: ISBN (1992).

²⁴ Society of Motion Picture and Television Engineers.

²⁵ See: SMPTE (2001).

Audio-visual Numbers (ISAN) for audio-visual material and Digital Object Identifiers (DOI) which is a generic content identification system²⁶).

4. Also important is the *identification of people* and organisations that intend to interact with the content. Not only does a rights owner need to associate a claim of ownership with the content but also the consumer will need to be uniquely identified. Such user identification systems are a prerequisite for DRM systems to be able to limit access to content to those users that have a right to gain access. One crucial aspect of the identification of *consumers* using unique identification schemes concerns Privacy regulations²⁷: When a DRM system uses a unique identification system for the consumers of content, it becomes fairly easy to generate a user profile that is potentially far more detailed than the ones credit card companies can assemble today. This is often seen as critical because the consumer has less control over such profiles when created by a service company located somewhere in the DRM value chain (from the rights owner via several intermediaries and service providers to the end user, see Figure 4) than if done by the credit card company that the user has a direct contract with.

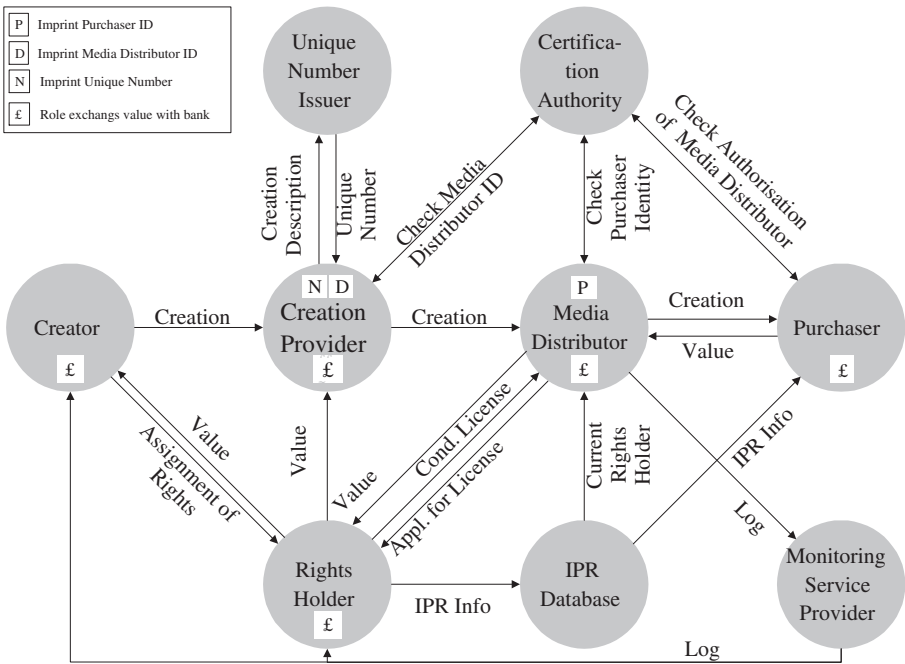


Fig. 4. A Model for a Content Value Chain: The Imprimatur Business Model²⁸

5. Closely related to the identification of people are algorithms to *authenticate* the person or organisation that wants to interact with any content. This function will involve cryptographic algorithms and may need an agency that issues electronic “passports” or certificates. This agency acts akin to the passport office of a country

²⁶ See: DOI (2003); *Paskin* within this book on page 26.

²⁷ See: Bygrave (2001); *Bygrave* within this book on page 418.

²⁸ See: Imprimatur (1997).

and is usually referred to as a “Trusted Third Party” or TTP as it is paramount that all members of the content value chain (see Figure 4) trust this party.

Only when the TTP is trusted by *all* parties in the content value chain, will the DRM systems and components that the TTP certifies be useable. It only takes one crucial partner to deny this trust for the whole chain to break and the DRM system to become useless in that particular value chain.

Other authentication needs can also be fulfilled by such algorithms with possible support from a TTP; two examples of such authentication are:

- Devices may need to authenticate themselves to the services they communicate with (and vice versa) so that both sides can be “sure” that they are communicating with a trusted member of the content value chain.
- Even within a DRM system, different components (e.g. the subsystem that deals with processing the rights expressions and the tools that “open” the secure container) need to establish a secure and authenticated channel amongst themselves.

A TTP may also perform a further task. When it is detected that a user or a component does not behave as expected (in other words: when the user or device cannot be trusted any longer)²⁹ it may be necessary that the certificate associated with that user or component is revoked. This revocation function is a crucial and hotly debated issue as device manufacturers do not like the idea that their devices may suddenly become unusable just because the TTP deemed it necessary to revoke some certificates.

6. Another set of technologies closely related to the identification of content are technologies to persistently associate identifiers and other information with the content³⁰. These most prominent technologies in this domain are *Watermarking* and *Fingerprinting*. In most cases, watermarking and fingerprinting is used to help to prove that a copyright violation has taken place. Hence these technologies are often referred to as forensic DRM technologies.

But both technologies also have non-forensic applications: Watermarking has, albeit with not too much success, been used to convey business rules to client devices. Examples include the Content Scrambling System (CSS) for Video DVDs and the SDMI³¹ Phase I watermark.

Fingerprinting has additional uses such as well. One example are services that automatically provide metadata to users from “listening” to the music. One use case often given is a user sitting in a pub or restaurant and, upon hearing a song he likes, activates his fingerprinting device (e.g. his mobile phone) which will recognise the song, and transmit some information to a service provider. When arriving at home, the user will find the same song as a DRM-governed audio file in his email inbox — sent by an automated system using the fingerprints to identify which song the user liked.

7. A mechanism to *report events* such as the purchase of a piece of content is also important in order to allow event-based payments to be processed. These event-based payments (e.g. “pay-per-view”) are one of the examples of new business models that DRM systems can enable.

²⁹ Reasons for such a loss in trust may be because a component type (or even an individual component) thought to be “secure” has been hacked.

³⁰ See: MPEG-21 PAT (2003).

³¹ Secure Digital Music Initiative.

Such event reports can also be of interest for organisations that are active in the collection of royalties, such as Collecting Societies (e.g. GEMA³² and GVL³³ in Germany).

8. *Payment systems* which are enabled through such event reporting systems need also to be integrated into the system. This involves either linking to a credit card or bank account, or to anonymous payment systems (often called “electronic cash”³⁴). However, both systems have problems associated with them: credit cards are, in many countries only available for adults, and electronic cash systems have not been able to attract enough users to make it worthwhile for a rights holder to accept this “currency”.

The final element³⁵ is the “glue” between the components listed above. Only through this glue, can participants in the content value chain trust the system to do what they expect it to do. Several DRM systems use *obfuscation techniques* to make the hardware and software that provide the DRM functionality resilient against reverse engineering and, more importantly, malicious attacks. Other systems use hardware support for providing the glue between different components. One example for such a system are products based on the Trusted Computing Platform Alliance’s (TCPA) specification³⁶. This specification is cited as an example for technology that has the ability to further the security and user–friendliness of DRM systems. On the other hand, the TCPA is often criticised for violating the privacy of users, as systems based on the TCPA have the potential to monitor *all* interaction between a user and his system³⁷.

IV Evaluation Criteria for DRM Systems

As indicated above, the various members of the content value chain (see Figure 4) will have different priorities as to what is important to them in a content distribution system. However, all have different interests and priorities in each of the following eight criteria: (1) how user–friendly is the system, (2) how trustworthy, (3) secure and (4) extensible is the system, (5) how can it be implemented, (6) what resources are needed for implementation and adoption, (7) how open is the system and, finally, does it (8) interoperate with other systems?

In the following subsections, these criteria are looked at in some detail. It is important to note, though, that they refer to the *entire content distribution system*, not the DRM subsystem, or even the DRM systems’ components.

IV.1 User Friendliness

User Friendliness is one of the most important criteria. The content distribution system and the DRM components that are a part of it have to be *very easy to use* for those participants in the value chain to access or manage content and rights. This is

³² Gesellschaft für musikalische Aufführungs– und mechanische Vervielfältigungsrechte.

³³ Gesellschaft zur Verwertung von Leistungsschutzrechten mbH.

³⁴ See: Asokan, Janson, Steiner, Waidner (1996).

³⁵ Of course, there are more than just nine elements that can make up DRM systems. Nevertheless the list presented here covers the most prominent and important components.

³⁶ See: TCPA (2002).

³⁷ See: Andersen (2003).

paramount especially for the consumer; why should a consumer switch to using a new system when it is cumbersome to use?

But the same argument is also true for other participants in the value chain. When there is an existing content distribution channel that offers all participants reliable revenue opportunities, why should those companies change to a new distribution method when this new method does not offer any benefits over the old one?

IV.2 Trust

The second criteria is the question of how far members of the value chain can trust the system to behave in the manner they expect. Rights holders especially will need to have enough trust in the system that it will not let their content “leak” out of the protective domain,³⁸ and that payment will be made in accordance with the business model defined for the content. At the other extreme of the value chain, the end user needs to be able to sure that access to the content in accordance with the rules agreed will be honoured.

Similar trust issues exist for the remaining participants in the value chain (e.g. payment system providers and fulfilment centres) and if they are not met, the system will not be supported by that member of the value chain. Depending on the importance of that member this may render the particular DRM unusable.

IV.3 Security

Security is the criterion that is most often listed as the top priority for DRM systems. Indeed it is important that a DRM system is secure, because it handles valuable goods — from the content itself to the money that consumers are willing to pay for it.

Recent investigations have shown that all DRM systems investigated can be broken into. Hence, none of the systems provide 100% protection against deliberate attacks.³⁹ DRM technology providers have long since acknowledged this fact and state that their systems can only be made impregnable at a fairly high cost: making the system significantly less user-friendly.

While it may be doubted that DRM systems can, in fact, be made as robust as it is sometimes claimed, one has to question, if this 100% protection is called for in the first place. As stated in Section II above, it makes no sense to secure content worth €5 using a lock costing €10. Following this argument, a DRM system needs to provide *adequate* security, not 100% security. Adequate from *all* involved parties’ perspectives, that is.

An entirely different aspect of security is the robustness of the DRM system when the content is illicitly removed from the secure container. Technology vendors of digital watermarks (which can, and often are, used in DRM systems) sometimes promise that their watermarks would survive such acts and that it would be possible to trace the content back to the person who illicitly took the content out of the container. Such functionality is often accompanied by a requirement to survive conversion of the content from the digital into the analogue domain.

³⁸ See: *Biddle, England, Peinado, Willman* within this book on page 344.

³⁹ See: Federrath (2002); *Hauser, Wenz* within this book on page 206.

IV.4 Extensibility and Flexibility

On-line distribution is a relatively new method of making content available to the consumer. It can therefore be expected that new business models will be tried — many unsuccessfully — in the next few years. It is therefore important that any DRM technology is flexible enough to deal with new ideas and concepts without costly upgrades. In that context, it needs to be taken into account that such new business models may be significantly more complex than today's relatively straight-forward subscription and "pay-per-view" models, and that they may be unimplementable on today's devices (with consequences with respect to the DRM system's implementability — see below).

Also, as the volume of DRM-protected content traded today is very small, it is important that the systems to handle the trading are able to "grow" with increasing demand. While it is unlikely that the DRM technology itself poses a limitation to such growth, the services built around DRM systems may hinder expansion and may need to be upgraded from time to time.

IV.5 Implementability

Of more interest to device manufacturers is knowing the resources needed to run a DRM system. The algorithms for a DRM system will tend to be chosen dependent on the type of device that the content is to be distributed for (is it a portable device, e.g. an ebook reader, with limited memory and processor power, or is it a desktop device such as a digital television set, or even a personal computer?)⁴⁰. It is the capacity of such devices that may severely limit the technical possibilities — and thereby the business possible models. Issues to look at include:

1. Memory requirements (RAM and ROM);
2. Processor cycles requirements;
3. Special hardware requirements (e.g. tamper resistant components, unique hardware identifier, ...);
4. Special software requirements (e.g. tamper resistant software modules, special operating system functions, ...), etc.

Also connectivity is an issue. If a DRM system needs a permanent connection to a server, the choice of types of devices which can be used for the such a DRM systems is significantly limited. This may not be a problem in some areas — and may even be part of a value-added service — but it will not work in other scenarios. For example a mobile music player that needs a constant connection to a server will not be usable when boarding an aeroplane as such radiating devices are not allowed to be switched on during flights.

IV.6 Openness

The requirement of openness has been discussed for quite a while⁴¹ and centres around the need for independent applications for accessing content (i.e. unprotected as well as DRM-governed content). It has been argued that allowing authors of shareware and open source programs⁴² to participate in the content value chain, will grow the appeal of such technology and systems and will lead to an increased use.

⁴⁰ This is because the DRM system is not the only component that needs to run on such devices.

⁴¹ See: Rump, Herre, Brandenburg, Koller, Allamanche (1999).

⁴² Which are, for example, widely used in the mp3 music environment today.

The major drawback of this openness would be that not only honest programmers would gain access to the specification but also those who are eager to provide applications that are written in order to circumvent any DRM system.

A possible way to achieve openness, while still being able to have closed and secure DRM system components, is to either formally standardise or openly declare the interfaces to such closed systems. When, in addition, the closed modules are available for a large number of different platforms and content types, shareware programmers could build their applications based on interfaces to such closed components.

IV.7 Interoperability

Closely related to user-friendliness and openness is the seventh evaluation criteria: To what extent does a DRM system *interoperate* with other systems. For example, when obtaining a DRM-protected ebook, does a consumer need to worry if it will be readable on his ebook reader at home? Or is some conversion needed? And, if so, how cumbersome (and costly) is this process?

Devices, services and content will need to be sufficiently interoperable for DRM protected content to gain widespread use, as it became evident with mp3 compressed music. While several attempts were made to distribute protected music, only a few DRM-enabled playback devices were available and — maybe even more crucial — different published recordings were protected by different DRM systems. This made it impossible to play records from content provider *X* on devices from consumer electronics manufacturer *Y*⁴³. The net result was (and still is) that most electronically distributed music is coded in mp3 *without* any protection. As there are plenty of “mp3 players” available on the market, the distribution of unprotected mp3s is inherently interoperable. Figure 5 illustrates who and what needs to be compatible with what when music is to be commercially distributed to mobile phones.

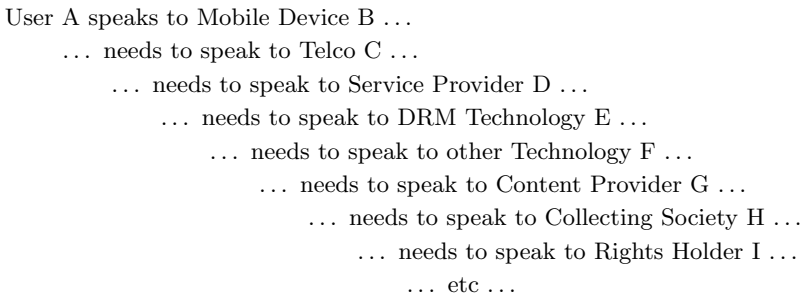


Fig. 5. Interoperability Chain

Developments such as the standardisation of interfaces to DRM systems as conducted by, for example, MPEG⁴⁴ with its MPEG-4 Intellectual Property Management and Protection⁴⁵, may offer the urgently needed interoperability between systems without prescribing the full system. DRM systems with open interfaces and components are, however, something security experts often warn against; and the breakdown of the Content Scrambling System (CSS) for DVD Video has proven that a fully-standardised DRM system does have its weaknesses.⁴⁶

⁴³ See: Rump, Herre, Brandenburg, Koller, Allamanche (1999).

⁴⁴ Ironically the same standards body that also standardised mp3 ...

⁴⁵ See: MPEG-4 IPMP Hooks (2001), MPEG-4 IPMPX (2002).

A completely different aspect of interoperability is the issue of upgrades. Does a DRM system, when upgraded (e.g. when new features are added or a security hole is plugged), provide backward compatibility? If not, how is the upgrade of the *content* a consumer has already obtained — and which, by virtue of the software upgrade, has become outdated — handled? If a user fears that the content he buys today becomes unusable tomorrow, he will certainly be very reluctant to spend any money. The same applies when the process of upgrading the content is cumbersome.

IV.8 Cost

Finally, the cost of a DRM system needs to be taken into account. The issues include:

1. The licensing cost for the underlying technology for the
 - a) Content provider's processes
 - b) Payment service provider processes
 - c) Manufacturer of devices that the end user is expected to purchase
2. The integration and implementation cost of the technology so that all affected members of the value chain become “DRM-enabled”
3. The cost to prepare the content elements for digital distribution. While this cost factor is often overlooked, this critical step includes, for example, ensuring that all rights have been cleared for the intended distribution.

As all such cost will, in the end, be paid for by the consumer, it is important that new distribution channels are more efficient, and therefore cheaper, than the old ones. Or, if additional cost is unavoidable, the introduction of new and *attractive* distribution channels may convince consumers to use — and pay for — DRM delivered content, and thereby DRM systems.

In addition, other members of the value chain such as equipment manufacturers will need to be convinced that licensing DRM system components and its integration into their devices is worth their while. In the mp3 case it seems that it would not be worth it: device manufacturers seem to be benefiting more from *not* implementing any DRM systems as mp3 players have become very popular appliances.

V Corporate DRM

Digital Rights Management is mostly associated with managing and protecting assets from publishers of ebooks, electronic magazines, electronic music, compressed and digitised films or videos, etc. However, DRM can be of assistance to *any* company or organisation that intends to protect its internal documents and memos from unauthorised access.

As such documents are content they can be protected from illicit access using the same DRM technology. For example, the annual report to be produced by the Managing Director of a company *A* may, before the report is published, be protected from being “read” by anyone but himself, the MD’s secretary and the members of the Board of Directors. Furthermore, only the MD’s secretary may “alter” the document and whenever she does this, an audit record will be created. At the time of publication, the access rights will be modified so that all of *A*’s employees and shareholders can “read” the document whilst there will be no “write” privileges any more. Parts of the document may even be made readable to people outside of *A* (such as journalists who

⁴⁶ See: Touretzky (2000).

may want to report on the financial situation of *A* but whom the MD may not want to disclose all details of *A*'s situation⁴⁷).

This corporate DRM example shows that the technology and the evaluation criteria discussed above also apply to the management and protection of “internal” assets of a company or organisation, albeit with a some differences:

1. The user friendliness of the system is of less significance as the company is able to force its employees to use a system even if it is cumbersome. Naturally, a user-friendly system would be beneficial as un-ergonomic components may lead to mistakes in the use of the system which, in turn, may lead to documents unintentionally leaking out.
2. Similarly, interoperability is not that important an issue in such cases because an organisation can simply select and prescribe the tools for internal use.
3. The integration of the DRM components into the existing infrastructure is, on the other hand, of higher importance as larger organisations will usually not have the ability to *replace* its systems. Such companies would need to upgrade and augment their existing system infrastructure.
4. Maybe even more important is the security and trustworthiness that the system provides. As the above example shows, the documents to be protected by the DRM system are likely to be of high value for the organisation and, therefore, it needs to be assured that the documents do not leave the secure container without approval (i.e. without a rights expression allowing this to happen).
5. A less important criterion is cost. Similar to “content companies” a cost-benefit analysis needs to be conducted. However, such an analysis is significantly easier to conduct when no consumer requirements need to be taken into account.

VI Conclusions

This paper provides an overview of the technical issues surrounding DRM and lists a variety of technologies that are needed to address several crucial aspects of digital content distribution.

But does DRM technology actually work? At the moment the answer might well be given with “no”. But a more careful appraisal might indicate that the real response has to be “we have not yet found the right business models and service offerings to make DRM worthwhile”. Clearly, this answer does not mean that DRM Technologies will not find their place in a digital commerce environment. It just means that there is still a lot to do.

VII Acknowledgements

The author wishes to thank the following people for helping in writing this article: Dirk Günnewig, Susanne Guth (who both feature in this book), my colleague Mark Isherwood and — last but not least — my wife Manon.

⁴⁷ This example also shows one crucial issue with DRM systems. They can only be as good as the weakest link (which may be a person using it): If an employee of *A* sells information he obtained from the DRM-protected report to a journalist, there are no technical means for the company can do to stop the journalist to publish the gained information. But, naturally, this “weakest link problem” also exists when no DRM system is used.

2.2 Requirements for DRM Systems

*Richard Gooch*⁴⁸

I Introduction — The Requirement for DRM

It seems apparent that the marketplace for entertainment products is diversifying in response to the technical possibilities for content distribution via the Internet. Research has been conducted and new business models have been proposed harnessing digital distribution to provide the consumer with new ways to access content⁴⁹. Examples include previews, rentals and so on. Far more flexible usage of content is also promised with the arrival of a plethora of new digital devices such as computers, portable digital audio players and entertainment servers in the home. Content providers recognise these trends as opportunities and have for some time been working to deliver market offerings as perceived opportunities emerge.

In order to deliver realistic products and services into market niches⁵⁰ created by the new technologies, it is first necessary to get the right marketing mix⁵¹. At a basic level this entails alternative options with different pricing and features, such as electronic delivery of previews, rentals and purchased products. But a service that lacks the means to prevent the use of, say, a rental as a purchased product, cannot then meaningfully offer these options as alternatives, let alone at different prices. DRM is not about locking up content, instead it is about unlocking alternative market offerings at different prices. Without DRM, access is literally *all-or-nothing* and all models in the middle ground are subsumed. DRM is required in order to offer a spectrum of services.

I.1 Mobility — The New Vernacular of Digital Devices

Beyond the delivery of alternative service options, the major application for DRM is in enabling the flexibility of content usage promised by digital devices. A novel aspect of new digital devices is that in the ordinary course of their functioning, these devices typically necessitate the transfer and storage of digital audio. For example, when content stored on a home-entertainment server is sent to a device such as a pocket player, copies of content are made, transferred and stored. Thus whereas the “copy” was at one time the unit by which products were sold, technology such as the above, has made the “copy” the unit by which digital products are consumed.

As in times past, the media format, player and the musical idiom are to some extent interlinked. A historical example is perhaps the vinyl disc, the hi-fi and the “concept album”. These conspired to produce a particular listening experience and there are

⁴⁸ Dr. Gooch is Deputy Director of Technology at IFPI, however this paper is written in a personal capacity and does not necessarily reflect the position of IFPI or its member companies.

⁴⁹ See: Jupiter Research (2002); Jupiter Research (2002b).

⁵⁰ While there is a very large base of content available over new Internet services, and some growing levels of commerce over these services, there are reasons why these new markets remain niche for the present. One powerful reason is that adequate Internet bandwidth is available only to a fraction of potential consumers of digital content services at present.

⁵¹ The term “Marketing Mix” is used here with a standard interpretation i.e. product, price, positioning and packaging.

other examples from chamber music right through to the compact cassette and “Walkman”. The advent of networked devices and extraordinary mobility of content is now linked with a “compilation culture” of music consumption⁵² where tracks are copied into archives on digital players and accessed via “playlists” rather than played direct from a physical product.

Rightsholders recognise benefits in new devices that allow new ways of consuming content. Specifically it is recognised that such functionality can only be delivered by “freeing” content from the physical carrier: obviously, the CD never was designed to physically fit into new portable digital audio players. But without some kind of “management” technology, devices lack the ability to discriminate between copying onto digital players (usually seen as desirable) vs. unlicensed copying over the open Internet. The latter has resulted in free-for-all copying that has been very prevalent but unhelpful for legitimate enterprise [see Tab. 1 below].

Unauthorised Internet Sites (Figs IFPI, Oct 2002)		
Web/FTP	200,000 pirate sites	100 million unauthorised music files

Peer to Peer Networks (Simultaneous users and files. Figs IFPI, Oct 2002)		
Service	Users	Files
KaZaA	2.74 million	481 million
iMesh	927,000	162 million
OpenNap (153 servers)	404,000	204 million
Gnutella (inc Morpheus)	112,000	19.6 million
All services	4.5 million	900 million

Tab. 1. Mass Copying and Dissemination Without Authorisation

Hence DRM must support flexibility not only in product offerings, but in their transportation, storage and access across a diverse range of devices. DRM is seen as offering greater access to digital items⁵³ albeit stopping short of totally uncontrolled access.

I.2 The Benefits of DRM

Taking stock, it is possible to summarise fundamental goals that DRM can help to deliver:

- Ability to offer *new delivery options* to the consumer, enabling network transfer to devices either as downloads or file transfers from a physical carrier
- Ability to meaningfully *offer different forms of access* at different price points, meeting increasingly diverse market demands such as preview, rental etc. as well as “buy to own”.
- *Mobility* to use content across diverse device types including hi-fi’s, home audio servers, pocket players, PC’s, PDA’s, mobile phones etc. without irresponsibly feeding the destructive phenomena of “free-for-all” copying.
- *Flexibility* to interactively access content e.g. through playlists.

⁵² This “compilation culture” is perhaps epitomised by the advertisement tagline from Apple Computer “Rip Mix and Burn” but certainly extends to music consumption via computer “jukeboxes” and many digital devices built around a “hard drive”.

⁵³ DRM offers greater flexibility of use than physical media because physical media is subject to physical constraints, while digital files are not.

These goals are driven by perceived market demand and the content providers desire to address that demand. For rightsholders there is a view that *wider understanding* of this need for DRM in the market is itself an important part of bringing such services to market.

I.3 The Environment for DRM

Naturally the whole enterprise of developing and delivering DRM depends on the extent to which a viable market is foreseen by those with capital to invest in developing the necessary infrastructure. Unbridled piracy and mass-copying [such as in Tabular 1 above] undermines the health and future prospects of the legitimate market. Therefore, in order to promote market potential and investment potential, it is essential to use all available means to clear a space in which legitimate business may grow and thrive, free from piracy. That task has certainly been grasped by rightsholder organisations. Various initiatives have been undertaken to tackle infringement and to promote a wider understanding of the role and purpose of copyright in the promotion of creativity and of investment in it.

I.4 DRM Technologies

Cryptographic techniques, whilst having a utility within DRM, cannot alone offer flexibility to accommodate different forms of content delivery and usage scenarios. Content must be packaged in forms that can be identified and accessed by playback equipment. This involved codecs, file-formats, metadata etc. Delivery should be possible via Internet or physical carrier. Internet delivery requires server systems and the whole gamut of e-commerce, security, authentication and delivery technologies. Delivery via physical carrier such as a CD may require technologies such as a hard-to-copy feature to prevent disc cloning, disc serialisation to permit Internet registration and either a self-contained player or an interface to player technologies already available on PCs and other target devices. Furthermore, if the disc is to be compatible with the largest base of player devices — CD players — then PCM audio must also be delivered, preferably with some form of protection. Several authors in this book deal more extensively with technologies that are required within DRM systems and extensive lists of DRM standards and initiatives compiled by NIST and CEN/ISSS⁵⁴.

But presently there is a lack of DRM implementations and there is even a lack of agreed definitions and nomenclature at many levels that continues to hinder technical discussion. This is a problem for rightsholders who seek rapid progress toward implementation. Rightsholders require the establishment of agreed nomenclature, at a general level and also at a detailed technical level. The recording industry is progressing the former in a wide range of fora, and the latter primarily within standards bodies.

By far the most promising and active area within which the recording industry is contributing to the evolution of DRM is MPEG (Moving Pictures Experts Group). MPEG is tremendously important because it is a forum in which technical experts from the various industry sectors meet and work, developing practical engineering standards. And MPEG has a track record of developing successful standards that are widely deployed⁵⁵. The recording industry is contributing to the MPEG IPMP work areas,

⁵⁴ See: NIST 500-241; CEN ISSS (2003a).

⁵⁵ MPEG standards are proven and have been influential in the design of digital delivery platforms in areas such as cable TV, satellite, Digital Radio and on the Internet.

in particular providing expertise in areas of Rights Expression Language (REL) and Rights Data Dictionary (RDD). These allow a means of expressing rules that are used within DRM and a defined meaning for the terms used in such expressions, respectively. Standardised RDD and REL will allow rules to be understood and processed consistently across content and hardware combinations from different vendors. In other words, this work provides the core solution to a fundamental requirement: *interoperability*.

II DRM Implementations in Software and Hardware

Clearly, DRM must be widely adopted if it is to find widespread use, and the deployment of DRM in players is interlinked with the availability of content in the appropriate format. It is not realistic to expect to deliver the one without availability of the other. There is a requirement for content, and for compatible players to play the content. Thus as a pragmatic measure, rightsholders have initially offered computer-based delivery and players where both the content and the player may be downloaded and installed on the personal computer.

Computer security is often criticised, based on many well-known examples of hacks, cracks and assorted infringing services on computers⁵⁶. Historically, computer-makers have failed to implement content-security mechanisms that have been used in devices such as CD players⁵⁷. In spite of this, the computer is actually an attractive platform within which to deploy DRM tools. The computer offers two significant features: the ability to download DRM-enabled tools and the ability to upgrade and renew security. As a consequence, many content services have to date been targeted at computers.

On the basis of such efforts a growing number of content sites and services are now offering a very large repertoire available for download via subscription or per track. For example, OD2⁵⁸ in Europe offers over 150,000 tracks from major and independent labels through retail partners such as HMV, FNAC, MSN and many others. Popfile.de was launched in Germany with over 20,000 tracks, and Pressplay has over 250,000 tracks. Listen.com has over 20,000 *whole albums* on their “Rhapsody” service.

A limitation is that computers are a small subset of the overall range of devices upon which consumers require to utilise content. There are two ways for content delivered via the computer to be “exported” for use on a wider range of devices. One way is to put the content into plaintext. The other way is to embed compatible DRM tools in devices. Clearly, the former would undermine the purpose of using DRM in the first place. The latter would achieve the purpose of making content accessible on such devices while providing the means to prevent indiscriminate exploitation such as uncontrolled copying.

Presently, all but an immeasurably small proportion of hardware devices shipped into the consumer market lack support for DRM tools⁵⁹. Lack of hardware support is a drawback for operators attempting to build a content distribution business on the Internet.

⁵⁶ One well-known example of a “crack” is the DeCSS software used to circumvent TPMs applied to DVD.

⁵⁷ Computer CD-ROM drives, for historical reasons, do not implement SCMS that was standardised for CD media and players. Nor do many computer drives appear to implement “RID” that was standardised in the “Orange Book” for CD-R devices.

⁵⁸ See: <http://www.ondemanddistribution.com>.

For such operators, the cost of setting up content servers and archives must be borne in full, whilst revenues can only be expected from that small sector of the consumer market equipped with devices to take advantage of the content offerings. And the situation will take time to improve. Until the vast base of CD players is augmented or replaced with DRM-capable devices, DRM offerings will remain a fraction of the overall market. Thus it is crucial to find ways to get DRM support *in hardware* and to get such hardware out into the market. Otherwise consumers will not have the means to take advantage of DRM-enabled offerings.

II.1 Interoperability

Interoperability and compatibility are terms that are frequently the subject of confusion. Compatibility merely means that different parts of a system can work together. Interoperability on the other hand is derived from military terminology describing the ability of troops and equipment to maintain a defined level of functionality during combined or joint operations. In terms of computing, interoperability is used to refer to components of computer systems that are able to function in different environments. For DRM a different environment in respect of a content service may take the form of a different player platform. In respect of a player device, a different environment may take the form of a different content service. Interoperability requires that a defined level of functionality is maintained both for security and “rendering” in such circumstances.

Interoperability is a fundamental goal for DRM systems. It is a characteristic that allows DRM to transcend the mere compatibility achieved by physical formats, whereby a disc will fit into the specified player. DRM should allow content to be accessible across the widest range of diverse device platforms from home-entertainment servers to pocket digital players.

A problem has been that, lacking hardware support for DRM formats, new services have been constrained for use only on the personal computer. This limitation was only partially solved when services allowed downloaded tracks to be burned to CD-Rs. This move undermines security and in no way lives up to the promise of file-based portability and flexibility offered by DRM systems. A complete solution requires adoption of support for DRM in a wide range of hardware devices. This process has begun with a number of devices either incorporating DRM support out of the box, or upgradeable with the necessary tools. In future, tools that can “affiliate”⁶⁰ devices on the home-network, are required so that content can be used flexibly across families of devices on the home-network but without offering scope for unauthorised distribution of that content over the open Internet.

Present hardware has not provided tools that can transform this vision of benefits of interoperability into reality.

⁵⁹ An estimated 800 million to 1.5 billion CD players have been shipped to consumers. This dwarfs the number of devices that support DRM. And many new digital players are still being shipped without any support for DRM.

⁶⁰ The term “affiliation” when applied to devices on a network should be understood as entailing registration of the devices so that they can be “trusted”. Once a device is affiliated, content can be sent over the network between that device and other affiliated devices, but cannot be sent to unaffiliated devices on the open Internet. The term can be used as a verb i.e. to “affiliate” a device, referring to the registration process.

II.2 Security

Once DRM is widely deployed in the marketplace, and is in use to protect traded goods of significant cumulative value, it can be expected that DRM will be subject to attack. A likely form of attack could be designed to gain unauthorised access to content, circumventing the protection or the access rules (though many other types of attack are also likely). The robustness of DRM against attack is a topic that deserves detailed consideration such as can only be provided using specialist security skills and techniques.

Security professionals have been split on this topic. Some authorities have argued that attempts to limit digital copying are futile⁶¹ though this does appear to be a minority view. Mainstream industry is actively researching DRM and building DRM into mainstream products⁶². One of the largest known commercial deals involving DRM involved the acquisition of Intertrust by a consortium including Sony and Philips. The deal was reported to be worth \$453 million and won regulatory approval from the European Commission⁶³. Furthermore, there is strong theoretical work on security within DRM systems⁶⁴. In spite of this body of work on DRM, it is clear that content providers and the security industry have not yet worked effectively together to achieve the levels of success seen in areas such as Pay TV, mobile phones etc.

Security professionals have developed a series of criteria that any technology must meet to offer credible security. Such criteria include:

- No global secret
- No single point of failure
- Renewability of security following a compromise or breach

It is realistic to ask that DRM can be designed to conform with these requirements, and in a form suitable for implementation in inexpensive consumer devices. Consumer appliances such as mobile telephones, set top boxes and computer–security tools are routinely designed and tested against such criteria. This does not mean that security will be impregnable. Rather, the goal is to design a system where one break does not render the entire system insecure. The approach set out in⁶⁵ advocates a risk–management approach to delivering cost–effective security in DRM applications.

On computers, content security cannot entirely be achieved by simply protecting content at source. When rendering content on a PC the content must be converted into a digital audio stream. In the current PC environment, it is impossible to ensure that the digital audio stream is routed to an output device, as opposed to being routed through a soundcard “emulation” and back to the hard drive in unprotected form. With modifications (e.g. the ability to reliably authenticate a physical soundcard) security on the computer could be dramatically improved. In fact the computer does offer one great advantage to assist security: it is possible to very easily renew and modify the security tools as often as needed, e.g. even part–way through a song. It is also possible to devise applications that, like an anti–virus checker, would scan the computer memory for traces of hostile applications that may be running. This opens a whole gamut of possible “active” security measures that could defeat pre–programmed circumvention tools.

⁶¹ See, e.g.: Schneier (2001); *Biddle, England, Peinado, Willman* within this book on page 344.

⁶² See: WM9–DRM; Helix DRM; EMMS.

⁶³ See: SPI.

⁶⁴ See: Kocher.

⁶⁵ See: Kocher.

As previously mentioned, PC-based services are vital to the early development and deployment of DRMs, and all the concerned industry sectors are working together developing different aspects of such tools. Rightsholders look forward to the delivery of security measures that seem likely to arise under IT-sector “trusted computing” initiatives such as Palladium, La Grande and TCPA.

In contrast to the flexibility and re-programmability of computer systems, hardware devices have to the present been inflexible, but less prone to hacking and circumvention. The present co-existence of a fixed, inflexible base of devices and formats together with re-programmable computers has proven to be the worst possible environment for security — exposing a single point of failure in the fixed format, but preventing wide market adoption of flexible computer security because it would be inherently incompatible with legacy devices. This situation is on the verge of changing as new hardware devices offering re-programmability (or at least, security renewability), begin to emerge. It will take time, however, for these devices to ripple through the market to an extent that allows the widespread adoption of DRM.

Security should not be obtrusive. DRM should function reliably in the background, and should not intrude on the user experience. This expectation is not unrealistic as many widely used tools, for example PC security tools such as VPN⁶⁶, have been engineered to offer reliable, un-intrusive services that offer a high level of security while supporting user requirements.

II.3 Legal Protection of TPM

Despite a generally improving outlook for DRM, technological protection measures used by DRMs are not immune from circumvention. There is in fact a trade-off between the complexity (and cost) of security measures employed and their efficacy in resisting attack, though no measure is un-hackable. In other words, the more pernicious and prevalent are tools for circumventing DRM, the greater the cost of designing and renewing protection measures within DRM. The more complex the DRM, the greater is the cost of running it on a device, either cost in processor cycles or battery life, or both. These costs will always be borne by the consumer purchasing protected content and devices for using it, though of course the consumer will not buy either unless benefits such as flexibility, portability and choice are significantly enhanced as a consequence of using these technologies. Thus it is of the utmost importance to the consumer and the market as a whole, to minimise costs associated with protection measures. One highly effective way to do this, is to minimise the extent to which DRM is subject to attack by putting in place strong legal protection against the circumvention of technical measures. This approach will minimise the security cost borne by the average consumer for tools that must be universally applied to defend against circumvention techniques implemented by the few circumvention experts.

Thus a fundamentally important aspect of DRM implementation concerns the balance between the strength (and cost) of technical protection measures within DRM vs. the extent to which attack methods are permitted (or at least the extent to which attacks are possible in practice). This balance is a matter of societal rather than technical prerogative, under the influence of legislators. Member States of WIPO agreed the 1996 “Internet” Treaties, which led to the adoption of the EC Copyright Directive, to address the unauthorized circumvention of technological measures and the manufacture and trafficking in illicit circumvention utilities.

⁶⁶ Virtual Private Network.

II.4 Privacy

A hypothetical pitfall that is often discussed concerns user privacy issues. It is sometimes said that DRM may, by virtue of authentication or key-management functions, be misused to accrue personal data. Of course misuse of any technology is possible, but such issues do not arise more significantly with DRM than with any other technology. In fact the core DRM would not normally be associated with personal data. Certainly DRM may exist alongside e-commerce systems that may store customer records, credit card details etc. but these system components are not actually a part of the DRM. The storage of personal data such as customer records is regulated in most territories and the presence of DRM running alongside such systems does not change that. For that data held within the DRM system (possibly including backup copies of “rights”, digital certificates or similar) it should be noted that DRM security serves to secure access to these components. Rightsholders and others building consumer-facing commerce systems want and need tools that allow for the proper compartmentalisation and protection of the various kinds of data held on those systems. Work towards that end is already occurring in the wider context of the development of e-commerce platforms and also in the legislature in key territories.

III Maintenance of DRMs

The longevity of different DRM versions (especially in respect to security) in the market and maintenance of old or obsolete DRM versions are of concern. Though standardization would go a long way to minimise such problems, these issues must be faced. Many devices are now designed to be upgradeable with new software being loaded to flash memory. One reason device-makers take this approach is to allow concurrent engineering of the hardware and software, but a benefit is the proliferation of upgradeable devices. Upgradability is not without limits however and it may be that obsolescence of content or devices is ultimately unavoidable — as it is in many fields. One example is computer software. When upgrading from 5 1/4” to 3 1/2” floppies, the older discs and drives rapidly became unusable and thus obsolete. DRM can potentially do better than this, since it may be possible to re-package content into new protected formats. At the very least, so long as these technologies are used to “buy” rather than simply rent or preview content, a requirement must be to have available proven and stable DRM technologies that will find extensive and long-term support in the marketplace.

III.1 Progress to Date

Clearly, there has been enormous activity and effort devoted to bringing DRM to market, and still some way to go. We may recount the advantages of DRM:

- Flexibility to deliver what the market wants, online and offline
- Means to differentiate services/uses allowing different price points
- Deliver totally new services like “advanced preview” or unlock bonus content for a different price
- Possibilities for interoperability/mobility much greater than present physical formats

At present there is increasing technology to deliver these benefits, with solutions being put in place, right through the value chain from licensing, production, protection, delivery, technology standards. Implementation is taking place across industry sectors covering the content industries, technology and hardware companies. At present, some less advanced implementations look more like simple Technical Protection Measures

than flexible DRM tools. Still, the goal is to build and deliver quality services, meeting market demand, and the better implementations are getting there.

Complete transition to DRM-enabled services will take time. Content is likely to be offered in legacy formats to the vast consumer base in support of their legacy players until these become totally obsolete. It does not seem reasonable to disenfranchise the owners of potentially 1.5 billion CD players by early adoption of technology that is incompatible with those players.

IV Summary

In concluding this paper, there are several points that can now be set out. Content providers see opportunities to offer alternative services that can be used more flexibly and the need for DRM results from that.

Of course there is also a need to prevent uncontrolled mass-copying. Technical Protection Measures are addressing that problem. But it is not enough to just have locks — to make a business one must offer access, convenience and a good user experience.

Overall, requirements have been highlighted in four distinct areas as follows:

Awareness. Whilst not directly an issue of DRM technology, there is nevertheless a requirement to:

- Promote awareness of the benefits of DRM
- Promote awareness of the role and purpose of copyright to stimulate creativity and investment

Development. Develop the functionality and flexibility of DRM tools:

- Develop flexible DRM systems that can support improved legitimate services handling a variety of content types
- Work towards interoperability via international standardisation e.g. within MPEG-21

Deployment. Deploy DRM so that services can be made available:

- Develop enhanced capabilities to provide a secure PC environment
- Ensure that DRM is embedded in a wide range of devices

Maintenance. Support DRM in order to maintain it's continued viability:

- Work to find solutions to gaps in protection that would otherwise threaten the development of a secure environment especially in regard to analog and legacy digital formats where these can be used as sources for unauthorised redistribution
- Provide capabilities to renew and upgrade security measures, especially following successful attacks against the security
- Tackle problems of unauthorised or unlawful copying and redistribution of copyright works. This is especially urgent in the context of P2P technologies. In tackling these problems, both legal and technical approaches are required

The rationale underlying these requirements has been elaborated through this paper. Previously, an almost identical set of requirements was drawn up during a DRM working group series organised by the Information Society Directorate-General of the European Commission held during November 2002⁶⁷. A question concerns the extent that governments should intervene in these matters.

Governments and authorities around the world have been helpful in supporting key industry fora such as MPEG and other standards initiatives. Fortunately, governments

⁶⁷ See: Directorate-General.

do not appear likely to “micro-manage” developments through more direct intervention at a technology level in order to deliver political objectives. That is not to say there is no role for government intervention, only that policy would normally concern the uses of technology and not the details of it. A very strongly worded view on this is given in: Schneier (2002)) although across the rightsholder communities (not to mention the technology sectors) there are a broader range of viewpoints.

As a final comment to this paper, it should be emphasised that DRM is a realistic and achievable development, absolutely necessary in the market for entertainment products, but also much more widely. But DRM is a long term proposition and there will be a need for much hard work and some patience.

2.3 Components of DRM Systems

2.3.1 Identification and Metadata

*Norman Paskin*⁶⁸

Abstract: Identifiers (unique labels for entities) and metadata (structured relationships between identified entities) are prerequisites for DRM. The term identifier can mean a label numbering scheme, specification, or fully implemented identifier system in a specific infrastructure. Implementations require a social infrastructure. In an automated environment, the entity being managed must be defined in a structured way, by means of attributes. Managed entities will often be abstractions, and the choice of which possible entities to distinguish as separable is not absolute but dependent upon function and context.

Interoperable DRM requires a persistent means of identification and structured description. Persistent identification can be aided by use of Internet technologies which allow indirection, separating names from attributes. Structured description requires an ontology framework, such as the indecs framework, which can support mappings using a managed data dictionary.

I The Practical Significance of Identifiers and Metadata in DRM

As commerce has become increasingly less dependent on the physical presence of both buyer and seller, means of identifying things uniquely and describing them unambiguously have become more and more important. The use of computers in mediating some aspects of the trading relationship has further accentuated this requirement. The near-universal adoption of “unique identifiers” such as the ISBN or the UPC/EAN barcode has been a direct consequence (and a precondition) for the development of EDI (electronic data interchange) and electronic trading.

The Internet, as it becomes a medium for trading in intellectual property, drives us several steps further. The digital network linking trading partners has for the first time to embrace consumers rather than simply supporting business-to-business transactions. The identity of the things that can be traded becomes much less clearly delineated when they may be computer files rather than physical objects. Users no longer have to access “content” only in pre-packaged products — it becomes possible to provide them with the precise customized package of content that they want (and which theoretically at least no one else may want). By the Internet we mean here the network of digital computers linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions, able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or other IP-compatible protocols; and providing high level services layered on that infrastructure⁶⁹; the

⁶⁸ International DOI Foundation.

⁶⁹ See: Kahn, Cerf (1999).

World Wide Web is only one such manifestation. In addition, many identifiers and metadata will be used in private, EDI, or other networks: hence a sound design principle is application independence: identifier and metadata structures should be independent of any specific technical expression.

In digital rights management (which I'm defining broadly here as the management of any rights, including those of non-digital entities, through digital means), we use digital representations of resources, parties, licences and other entities (digital objects) to articulate a property system. One of the most important things a formal property system does is transform assets from a less accessible condition to a more accessible condition, so that they can do additional work. Unlike physical assets, representations are easily combined, divided, mobilized, and used to stimulate business deals. By uncoupling the economic features of an asset from their rigid, physical state, a representation makes the asset "fungible" — able to be fashioned to suit practically any transaction⁷⁰. Digital objects may also directly represent value⁷¹, though for current DRM purposes we are largely content to have DRM technologies work with normal currency mechanisms — concepts such as DigiCash, Beenz and the like have not (yet) found success.

The management of the myriad transactions implicit in such a complex network environment will only be possible if mediated by computer systems. This puts additional pressure on the requirement for unambiguous identification and description of the content through metadata. Persistent identification and description is a prerequisite for the management of intellectual property rights in the digital environment. Whilst identification of content is the most advanced area — perhaps because in many ways the easiest — the same principles apply to identification of all entities involved in rights transactions: parties, resources and agreements, as described in the indecs (interoperability of data in e-commerce) model of commerce⁷². The indecs framework has been widely recognised as a significant contribution to understanding metadata in the context of DRM, and the present article draws heavily on the indecs work and its implementation in the Digital Object Identifier⁷³, though the principles discussed, and conclusions drawn, are independent of any specific application.

II The Relationship of Identifiers and Metadata

Identifiers and metadata are two sides of the same coin. An *identifier* is an unambiguous string denoting an entity; an *item of metadata* is a relationship that someone claims to exist between two entities, each of which may have an identifier (and must, in an automated environment). These entities may include both objects and concepts: e.g. an item of metadata may be "this book has a

⁷⁰ See: De Soto (2000).

⁷¹ See: Kahn, Lyons (2001).

⁷² See: Rust, Bide (2000).

⁷³ See: DOI (2003).

cover coloured blue”, and that blue may be specifically identified by a Pantone number; both the book and “blue” would be identified entities. *Entity* is a term used to mean simply something that is identified. The underlying idea, from the <indec> project, is that nothing exists in any useful sense until it is identified.

An *ontology* is a tool which is able to structure relationships between entities; an explicit formal specification of how to represent the entities that are assumed to exist in some area of interest and the relationships that hold among them⁷⁴.

III Identifiers

An identifier is an unambiguous string or “label” that specifies an entity (something that is identified). Note that the term “identifier” has become rather overloaded and is used synonymously for several related concepts; discussed in more detail in section V. In computer science terms, an identifier is a name; the entities named occupy a specific domain of application (the namespace) and are points in that namespace. “*Naming is one of the most important and most frequently overlooked areas of computer science. In computing it is rumoured: everything is a naming problem*”⁷⁵. Once points in a name space are addressable, applications can be constructed which provide links (i.e. denote relationships) into the namespace or between points, to express metadata. Identifiers assigned to intellectual property entities would enable connections to be denoted (at an intellectual level and in practical terms for trading) between entities which are physically separated, which may be abstract properties, or are the product of separate authors etc.

The principal reason for assigning identifiers to points in a namespace is to realise that abstract namespace as a real digital environment (addresses in a network or computer system), which can then be readily manipulated. Information expressed in a digital manifestation is a Digital Object: “*a data structure whose principal components are digital material, or data, plus a unique identifier for this material*”⁷⁶. “*A digital object is not merely a sequence of bits or symbols [...] it has a structure that allows it to be identified and its content to be organized and protected [...]*”⁷⁷. These definitions capture the idea that a digital object is a meaningful piece of data, reflected in other descriptions such as DLO (Document–Like Objects)⁷⁸ or KNOBs (Knowledge Objects)⁷⁹.

From the standpoint of intellectual property or “content”, an Object is a digital subset of a greater class of entities, Creations (products of human imagination and/or endeavour in which rights exist) encompassing in addition to digital objects, physical packages, spatio–temporal performances, and abstract works.

⁷⁴ See: Sowa (2000).

⁷⁵ See: Irlam (1995).

⁷⁶ See: Kahn, Wilensky (1995).

⁷⁷ See: Cross Industry Working Team (1997).

⁷⁸ See: Caplan (1995).

⁷⁹ See: Kelly (1997).

Intellectual property — broadly, “works of human intellect or imagination” — can be formally defined in an ontology such as indecs, but where possible the analysis references definitions agreed by the World Intellectual Property Organization and related international treaties like the Berne Convention. These Creations may each have applicable namespaces, not all of which have digital realisations. From the standpoint of the Internet, a Digital Object is a Resource as specified in the Uniform Resource naming schemes.

IV Unique Identification

Uniqueness is the essential attribute of an identifier, which must be unambiguous in the defined namespace: a given identifier must specify (be bound to) one and only one object in that space. This does not imply that one object may have only one identifier (a one-to-one relationship), since a one-to-many relationship (an entity having several labels, each unambiguously specifying it) may be necessary in some contexts, and is likely in many DRM applications: as multimedia entities become more complex, or parties such as publishers operate in multi-media, multi-national environments, it becomes inevitable that they will acquire more and more domain identifiers, which may or may not require reconciliation. The question of whether — or how — different identifiers for the same entity should be reconciled is both practical and political. The multiple labels may be valid in different namespaces to guarantee interoperability (e.g. a sound clip within a multimedia scientific document may have one identifier within a music identification scheme, another identifier within a document archive); or the multiple identifiers may be within the same namespace, perhaps for pragmatic reasons beyond the abstract design of the namespace.

The indecs *Principle of Unique Identification* is that “every entity should be uniquely identified within an identified namespace”. It is difficult to overstate the importance of this simple and commonplace principle. At one level it can be said that the basis of interoperable metadata is simply about the relationships of recognisably unique identifiers. In pre-digital bibliographic and commerce systems, effectiveness depends to a great extent on the robustness of their identification systems: the UPC/EAN product numbers, the ISBN book identifier and the CAE composer/author/publisher identifier are among the most successful identification systems in use in the world of content management; they form the backbone of highly effective distribution systems in their respective industries.

In contrast, where unique identifiers for major entities do not exist or are poorly implemented within a domain, data management costs are higher — and simple, effective management systems difficult to develop. The absence of unique “party” identifiers for creators and publishers in the major content industries, the scarcely visible implementation of the ISRC for sound recordings, and the lack of a standard agreement or licence identifier in any copyright community, are each examples of gaps that are crippling for interoperability within a domain, let alone between traditional domains. Some of these gaps are now being

filled: e.g. the InterParty project⁸⁰ is providing one way of approaching party identification, by investigating a framework to make existing party identifiers interoperable.

Multi-media, multi-lingual, multi-national, multi-purpose metadata also requires that unique identification applies at all levels, including the use of “controlled vocabularies” for values of properties such as measures, form and type. In truly well-formed metadata, the only “free text” properties of an entity are found in its names or titles; in some instances (for example, in trademarks and in the UK Actors registry Equity), even names may be protected to ensure their uniqueness in a given domain.

For wider interoperability, the most important properties of an identifier are uniqueness within a given domain; stability (identifiers should never be transferred to another entity); security, whether through protection by watermarking or encryption, and/or by internal consistency through the use of check digit algorithms; and the public availability of some basic descriptive metadata for the entity identified, without which the identifier has only limited use.

V Identifiers as Numbering Schemes, Specifications, and Identifier Systems

We need to make an important terminology distinction at this point about the use of the word “identifier”. As the use of numbering in digital networks has developed, the historical use of the word in this context has become expanded to the point where it is now used synonymously to cover several different things, all of which are useful but which actually carry different implications that need to be separated in a detailed understanding of practical DRM applications. It’s important to understand the differences here; and to note that these are not mutually exclusive (one particular “identifier” may fit into one or all of these categories).

V.1 Identifiers as “Labels”: The Output of Numbering Schemes

A numbering scheme is a formal standard, an industry convention, or an arbitrary internal system such as a an incremented production serial number etc., to arrive at a consistent syntax for denoting and distinguishing separate members of a class of entities⁸¹. The scheme is a specification for generating a number: this resulting “number” may include alphanumeric characters, but the accepted parlance is to speak of these as numbers (e.g. ISBN = International Standard Book Number). The intent is of establishing a one-to-one correspondence between the members of a set of labels (numbers), and the members of the set counted and labelled. The product of the process is enumeration, a cardinality judgement, and assigned numbers for each cardinal member. An example

⁸⁰ The InterParty Project Web Site: <http://www.interparty.org>.

⁸¹ See: Ehlers (1994).

would be the ISBN, where a separate ISBN is assigned to each book edition. The numbering scheme may or may not be accompanied by some apparatus — for example, a registration agency and maintenance agency for the ISO TC 46 series of identifiers.

The important point here is that the resulting number is simply a label string (a “noun”). It does not of itself create a string that is actionable in a digital or physical environment (a “verb”) without further steps being taken. It may be used (and probably will be used) in databases; or it may be incorporated into another mechanism later.

The most common standard numbering schemes of interest in DRM include those standardised by ISO⁸²:

- ISBN: ISO 2108:1992 International Standard Book Numbering (ISBN)⁸⁴
- ISSN: ISO 3297:1998 International Standard Serial Number (ISSN)⁸⁵
- ISRC: ISO 3901:2001 International Standard Recording Code (ISRC)⁸⁶
- ISRN: ISO 10444:1997 International Standard Technical Report Number (ISRN)⁸⁷
- ISMN: ISO 10957:1993 International Standard Music Number (ISMN)⁸⁸
- ISWC: ISO 15707:2001 International Standard Musical Work Code (ISWC)⁸⁹
- ISAN: Draft ISO 15706: International Standard Audiovisual Number (ISAN)⁹⁰
- V-ISAN: Draft ISO 20925: Version Identifier for audiovisual works (V-ISAN)⁹¹
- ISTC: Draft ISO 21047: International Standard Text Code (ISTC)⁹²

Whilst these ISO TC46 identifiers were originally simple numbering schemes, of late they have also begun to adopt the notion of associating some minimal structured descriptive metadata with the identifier. Also relevant are the ISO-affiliated NISO standards including:

- ANSI/NISO Z39.84 The Digital Object Identifier⁹³

⁸² See: ISO TC49/SC9⁸³ — Information and Documentation — Identification and Description Standardization of information identifiers, description and associated metadata and models for use in information organizations (including libraries, museums and archives) and the content industries (including publishing and other content producers and providers).

⁸³ Available at: <http://www.nlc-bnc.ca/iso/tc46sc9/>.

⁸⁴ See: ISBN (1992).

⁸⁵ See: ISBN (1998).

⁸⁶ See: ISRC (2001).

⁸⁷ See: ISRN (1997).

⁸⁸ See: ISMN (1993).

⁸⁹ See: ISWC (2001).

⁹⁰ See: ISAN.

⁹¹ See: V-ISAN.

⁹² See: ISTC.

⁹³ See: ANSI/NISO (2000).

V.2 Identifiers as “Infrastructure Specifications”: Making Labels Actionable

“Identifier” is also sometimes used to mean a mechanism or syntax by which any label (as defined above) can be expressed in a form suitable for use with a specific infrastructure tool. This is sometimes known as creating an “actionable identifier” — meaning that in the context of that particular piece of infrastructure, the label can now be used to perform some action: e.g. in an internet Web browser, it can be “clicked on” and some action takes place.

Of particular relevance for DRM, the set of internet specifications known as Uniform Resource Identifiers (embracing URLs and URNs) provide mechanisms for taking labels and specifying them as actionable within the internet. These are discussed in more detail later in this paper — here we simply note the functionality that such systems are intended to provide. The same principles can apply in the physical as well as internet environment — for example by prefixing an ISBN with the EAN sequence 978 or 979, the ISBN becomes a UPC/EAN identifier expressible as a physical bar code symbol, or a radio-frequency tag, for use in the physical supply chain⁹⁴.

Importantly, note here that such “identifiers” do not mandate a way of creating labels, they merely accept any labels: hence if one does not have an existing numbering scheme, it will be necessary to adopt or create one in order to form URIs. A URI specification merely ensures that a label follows the rules to become actionable in an Internet environment: a specification is not an implementation, with all the other aspects that a fully functioning identifier system (see below) may require: URI may for example specify the syntax, and specify a recording registration procedure, but not create a managed environment (e.g. by which registrations are “policed”), or carry any specifications of metadata or policy (which I consider to be the hallmark of a full *identifier system*). Some identifier specifications of this form may have limited rules or requirements for implementation: so far this is limited to the URN specification including a proposed (not implemented) mechanism for resolution. The acid test one should ask of such a specification is: *what does specifying my label in this particular form get me, in practical terms, in a specific infrastructure?*

V.3 Identifiers as “Implemented Systems”: Implementing Labels in an Infrastructure Environment

The UPC/EAN is an “identifier system” in the physical supply chain; a DOI is an “identifier system” in the digital supply chain. ISBNs for example become implemented in the physical supply chain through UPC/EAN bar codes or RfID tags. This sense of “Identifier” denotes a fully implemented identification mechanism that includes the ability to incorporate labels, conforms to an infrastructure specification, and adds to these practical tools for implementation such as registration processes, structured interoperable metadata, and a policy/governance mechanism. Such a system is necessary for practical DRM

⁹⁴ See: Osborne (2002).

applications; since DRM deals with digital entities, structured metadata will be an essential component of such a system. The DOI is one of the better developed, with several million DOIs currently in use by several hundred organisations.

Both ISO TC 46 and URN have published suggested lists of requirements for their identifiers — the first covering what I have called here “labels”, the second what I have called “infrastructure specifications”. I have summarised these elsewhere⁹⁵ and suggested that a practical *identifier system* (which builds on both concepts) for digital use (DRM) should assume a combination:

- Unique “dumb” identification: unambiguous simple identification (label assignment) of a defined piece of information; opaque strings, not hard-wired with any specific application intelligence;
- Well-formed metadata: defined namespaces and controlled values within those namespaces for each value of a metadata element, defined by inherent structure not by their function in a particular application. A means of expressing an ontology to facilitate interoperability in many different functional applications;
- Support for arbitrary levels of granularity;
- Multiple, co-existing, labeling schemes should be possible, including support of existing (legacy) schemes; groups of content owners with common interests should be able to devise their own schemes which should then be interoperable in an open framework; multiple (overlapping) identification of content must be allowable. This implies extensibility: the ability to add within a scheme a particular namespace that defines that element.
- Links to distributed metadata: dumb identifiers pointing to specific repositories for different pieces of data, relating to different functions e.g. copyright, trading, EDI; details of medium, version, format etc. conveyed as metadata;
- Distributed (cascading) administration responsibility: once below a certain level, no central agency permission needed to assign unique numbers (sub-levels assigned by the owner of the higher level);
- Policy and governance process: a management structure design for the practical operation of the identifier registration and maintenance processes.

The three uses of the word “identifier” (*label*, *infrastructure specification*, and *implementation*) can become easily confused, since one particular string can be in more than one category. But to see why we need to be precise, consider the following statement:

“For use on the Internet, an ISBN label can become a URN specification; an ISBN label can be incorporated into a DOI, which is an implemented identifier system following the URI specification.”

Replacing the more precise terms in this statement by the loose unqualified synonym “identifier” results in confusion:

“an ISBN identifier can become a URN identifier; an ISBN identifier can be incorporated into a Digital Object identifier, which is an implemented URI identifier”

(true, but only on close textual analysis!).

⁹⁵ See: Paskin (1999).

VI Social Infrastructure and Costs

Creating an implemented identifier system for DRM is not a trivial task: it necessarily incurs some costs, in three principle areas:

- “label” registration; maintenance of resolution destination(s); declaration of metadata; validation of number syntax and of metadata; liaison with the registry; customer guidance and outreach; marketing; administration
- Infrastructure: resolution service maintenance, metadata registry maintenance, and further development
- Governance: common “rules of the road”; business model for cost recovery, development of the system

There is a widespread recognition of the advantages of assigning identifiers (labels); and of making these actionable; and a widespread misconception that an abstract infrastructure specification (like a URN or URI) actually delivers a working system rather than a namespace that still needs to be populated and managed. A common misperception is that one can have such a system at no cost. It is inescapable that a cost is associated with managing persistence and assigning identifiers and data to the standards needed to ensure long-term stability for DRM. This is because of the need for human intervention and support of an infrastructure. Assigning a library catalogue record, for example, will typically cost anything up to \$25. Assigning an ISBN or ISSN or National Bibliography Numbers will also have costs, even if these are not paid directly by the assigner. The most widespread model of recovering costs is from the assigner community: the DOI as an example is free at the point of use, but there is a small fee to an assigner for creating a DOI (a few cents) because the model chosen is that of a self-funding system (on the model of the UPC/EAN system).

Understanding identifiers in the digital world is fraught with such misunderstandings: “adding a URL costs nothing” (which itself ignores some infrastructure costs), “so why should assigning a name have a cost?” It is indeed possible to use any string, assigned by anyone, as a name; but to be useful and reliable any name must be supported by a social as well as technical infrastructure that defines its properties and utilities. URLs for example have a clear technical infrastructure (standards for how they are made), but a very loose social infrastructure: anyone can create them, with the result that they are unreliable alone for long term stable use as they have no guarantee of persistence let alone associated structured metadata. UPC/EAN product codes, Visa numbers, and DOIs have a tighter social (business) infrastructure, with rules and regulations, costs of maintaining and policing data — and corresponding benefits of quality and reliability. When a credit card is presented, we can be reasonably certain that the number is valid, and has been issued only after careful correlation with associated metadata by the registrant. It does not necessarily imply a centralised system: it may be a distributed system (like domain names), but it must have some form of regulation.

Such regulation of infrastructure for a community benefits all its members; funding the development of it is often a problem, and there is no “one size fits all”

solution to how this should be done. But finding a workable model for the development of an infrastructure can yield obvious benefits. There are many modern examples (3G telephone networks, railways) which are struggling with the right model for supporting a common infrastructure. The Internet was largely a creation of central (US) government; the product bar code, a creation of a commercial consortium. Product codes, Visa numbers, and DOI for example use the concept of Registration Agencies, rather than relying on centralised subsidy. These Agencies effectively hold a “franchise”: in exchange for a fee to the governing body, and a commitment to follow the ground rules of the system, they are free to build their own offerings to a particular community, adding value services on top of identifier registration and charging fees for participation.

Identifiers may of course be made available at “no charge”, if the costs of doing so can be met from elsewhere (there is no such thing as “free”, only “alternatively funded”). Like any other piece of infrastructure, an identifier system that adds value (like metadata and resolution) must be paid for eventually by someone. An organization could, if it wished, assign identifiers freely (registration fee zero to registrants) and subsidize this added-value service by paying a franchise fee to the governing body from a central fund, as an acceptable cost for supporting the service.

VII Namespaces as a Way of Managing Identifiers

The development of domains or namespaces within the Internet has helped in the relaxation of pressure on the need for absolute uniqueness in the structure an identifier: URIs provide specifications for universal disambiguation that allow even common terms to assume unique, network-wide, status.

A namespace is a set of names in which all names are unique. While one is working within one namespace, uniqueness is by definition not a problem. A potential problem arises when two namespaces containing the same label (but for different entities) are made interoperable. This is the issue faced by e.g. merging of databases. Namespaces allow reference to each label in the form `mid:nss` (namespace identifier: namespace specific string), so that the full string includes both an identifier of the namespace and the specific string within that namespace. This is the solution adopted within URNs and by XML, which has popularised the concept over the past few years. XML namespaces provide a simple method for qualifying element and attribute names used in Extensible Mark-up Language documents by associating them with namespaces identified by URI references⁹⁶. The XML namespaces recommendation works, but a number of underlying issues (e.g. validation) remain unclear⁹⁷. Nevertheless XML is the de facto standard way of communicating data and highly advisable for any identifier/metadata scheme to make its elements available in this form.

⁹⁶ See: W3C (1999).

⁹⁷ See: Bourret (2000).

However, we are far from having all DRM transactions automated, and although this is a logical solution if every transaction was fully and precisely specified, in practice if a particular community is working in one namespace, or using less formal methods, it will usually assume “nid” to be implicit — which brings problems when two namespaces need to be considered. A practical example is the author identified as “Joan Brady” — in fact, a different person in the “UK author namespace” (a Whitbread Prize novelist) and in the “US author namespace” (author of “God on a Harley”): in effect, these undeclared namespaces collide on an Amazon.com search, resulting in confusion and ultimately threats of litigation⁹⁸.

There is no fundamental logical difference between a “name” and “an address” — an address is the name of a location, i.e. a name in a namespace consisting of addresses (e.g. the URL namespace). But this does not mean that addresses can always be used as useful names: in DRM, a requirement is to manage entities (resources, parties etc.) as “first class objects” — that is, named entities in their own right — not via a property (location) which may vary independently of the entity.

VIII Abstractions

In most cases when an intellectual property entity is identified, the entity being identified is not tangible, but an abstraction. Clearly this is the case when identifying abstractions such as the underlying work “Robinson Crusoe” which has many different manifestations as book editions, or “Eroica symphony” in many recordings, scores, and performance. Not as readily appreciated is that apparently “tangible” entities are also abstractions: e.g. the ISBN identifies not the copy of a book which you have in your hand, but the class of all such copies, an abstraction.

Abstractions need an ontology to make sense of them. More than one ontology can provide tools for dealing with any set of entities, but we need to be careful not to mix definitions from different ontologies without careful mapping: every schema has its own inherent contextual model and its elements are defined in those terms. For example, there is a fundamental difference in the way in which the library-derived FRBR model⁹⁹ defines the term “expression” and the way <indecs> defines “expression”, but this is not to say that only one is right: each recognizes the entity that the other is calling “an expression” and wishes that the other had called it “foo”. Mapping elements is a completely different and much more complex process than declaring data elements. The indecs/DOI/ONIX group, for example, can map more or less any other schema successfully within their models, but we would not assume that any other schema would adopt the same definitions of (say) agent, resource or event. It has been well said that “there are more abstractions than are ever conceived of”.

⁹⁸ See: Bide (1999).

⁹⁹ See: IFLA (1998).

IX Identity and Sameness

A fundamental purpose of identifiers is to define when two things are “the same” and hence denoted by the same identifier. The intuitive meaning of “the same” needs some logical analysis if it is to be applied consistently for automation. The word ‘same’ is used sometimes to indicate similarity (qualitative sameness), as in ‘*Alice is the same age as Bob, and the same height as last year*’, sometimes to indicate that what is named twice should be counted once (numerical sameness), as in ‘*the morning star and the evening star are the same planet*’. The word ‘identical’ can also have the former sense (identical twins, identical dresses) as well as the latter; hence philosophers are liable to discuss both kinds of sameness under the label ‘identity’. Qualitative sameness is a comparison of metadata: entity A and B share a relationship to entity C. Numerical sameness is a simple logical relation through comparison of identifiers, in which each thing stands only to itself. “*Although everything is what it is and not anything else, philosophers try to formulate more precisely the criteria by means of which we may be sure that one and the same thing is cognised under two different descriptions or at two distinct times*”.¹⁰⁰

Numerical sameness leads to a trap for the unwary: if we say, “Two entities are the same if they have the same identifier,” we seem to create a puzzle: how can they be two if they are the same? If identity is a relation it must hold either between two distinct things or between a thing and itself. To say that A is the same as B, when A and B are distinct, is bound to be false; but to say that A is the same as A is to utter a tautology. Different solutions have been found by different philosophers for this “paradox of identity”. This may seem like remote philosophising, but in fact lies at the heart of practical implementations.

In determining whether A is the same as B, we find that ultimately nothing is the same as something else; however, it makes sense to consider that A is the same as B *for a defined purpose* (i.e. in a defined context). To give a practical example, a photocopy of this article is not the same as the original in some ways (it is printed on different paper stock, it is located in a different part of space, etc.); but it might be considered the same — a copy — *for the purposes of intellectual property* (it retains the typographical layout and semantic sense). Here, the attribute “paper stock” is irrelevant, the attribute “manifestation of the defined work X” is relevant, for the purpose of DRM. Whilst this seems almost trivial in a physical environment, where the purpose and context are intuitively understood even if not stated, in a fully automated digital environment the attributes and context are less intuitive. This is why it is difficult to translate intuitive concepts from the physical world into the digital; e.g. arriving at a definition of “to copy” in the digital environment makes no sense without a context. In recent MPEG-21 discussions, some technologists argued that there can be “no such thing as a digital copy” — A and B must differ because of the sequence in which their data representations are laid down on a hard disk, for example. Yet it clearly is nonsense to say that “the action of copying is impossible in the digital domain”:

¹⁰⁰ See: Kemerling (2002).

this would undermine copyright law as rampant copying is patently occurring in practice. Hard disk sequencing is an irrelevant attribute *for the purpose of* IP law — though case law in this area is sparse — and similarly, in more traditional IP interests, photocopier technologists are not ideal intellectual property lawyers.

So it is meaningless to ask “Are A & B the same thing?” and only meaningful to ask “Are A & B the same thing for the purpose of...”. Technically we do this by considering which attributes of A need to be retained in creating the replica B; some attributes are ignored, considered irrelevant for some defined purpose. A description is a set of properties that apply to a certain object: two incomplete descriptions denote the same object if they have an identifying property in common¹⁰¹; the descriptions are for a purpose, and the “identifying property” (or more likely set of properties) is the one by which we define that common purpose or context of the A and B comparison.

When we make statements we normally leave a great many attributes unstated because we assume general or specific knowledge on the part of our audience. However when we come to fully automated DRM, which relies on exchange between computer systems, we cannot expect that any inferences from “common knowledge” will be applied. We need to consider an entity as no more than the sum of its stated attributes. I may say you can copy my CD and its entire contents and sell it in a jewel box: exactly what kind of jewel box, and what the printing on the CD and the inlay says is irrelevant to the copy. It is a replica if the stated attributes are the same at whatever level of granularity is explicit. It may even be a copy if it is not a CD, if the only stated attribute I have given is “this recording”. DRM will rely on the same principle as any other computer system: computers are dumb, and if something is not specified it cannot be taken into account.

The same principle of considering a comparison *relevant for some purpose* applies to the use of metadata in automated applications: we must sort the metadata into sets (application profiles) which are relevant for the particular purpose of that application. As Karl Popper elucidated, there is no neutral purpose-free “*tabula rasa*”, always a purpose which is inherent in a particular act of perception¹⁰². The recognition that all considerations of identity require recognition of context is fundamental to the context model underlying the *indecs Data Dictionary* (which will be discussed later in this paper), in which all are things are ultimately part of events or situations, taking place in defined contexts.

X Granularity

The paradox of identity is related to the concept of recognising granularity. Recognising sameness among a population, as we have seen, depends on choosing which particular set of attributes of a number of entities we consider relevant, and which are irrelevant, and ordering the population into sets defined by the relevant attributes for the purpose in hand.

¹⁰¹ See: Guarino, Welty (2000).

¹⁰² See: Popper (1972).

Granularity refers to the level of content detail identified; and to this we must add again the qualifier “identified for a particular purpose”. To take an example from text publishing, the ISBN¹⁰³ identifies the whole book; the BICI¹⁰⁴ identifies component parts of a book (e.g. chapters, sections, illustrations, tables). This may be enough for some uses but is clearly inadequate for others. If we are to be able to identify all rights owners in a particular piece of content, that may require a far finer degree of granularity of identification, to the level of the individual illustration or quotation from another source. Similarly, if information is to be traded with customers at a level of granularity finer than the “chapter” or the “article”, then publishers may have compelling marketing reasons for being able properly to identify and to keep track of what is being traded.

The level of granularity that may need to be identified becomes effectively arbitrary in a digital environment. This might suggest a requirement for relational identification where (like the BICI) smaller fragments are identified by reference to the larger “whole” from which they come, although this “intelligence” would have some drawbacks, not least in terms of the size and structure of the codes and a preferable route would be to express the relationship through readily accessible metadata. Considerations of granularity are fundamental to a logical analysis of DRM, and a key point is the purpose and context of the granularity choice.

X.1 Functional Granularity

The index *Principle of Functional Granularity* is that “it should be possible to identify an entity whenever it needs to be distinguished.” When should an identifier be issued? In this deceptively simple question lies the most basic question of metadata: for which data is it meta-? Resources can be viewed in an infinite number of complex ways. Taking the index metadata framework document as an example, it has an identifier in the <index> domain: WP1a-006-2.0. But to what does this refer? Does it refer to the original Word document, or to a pdf version available on the Website? Or does it refer to the underlying “abstract” content irrespective of delivery format? If it refers to the Web document, is this also adequate as a reference to local copies that have been downloaded onto other computers or servers? The document’s parts may require identification at any level (for example, section 2.2, or Diagram 14). If you wish to make a precise reference to a sentence from another document, you will need a more precise locator, and its nature will depend on whether your reference is intended to allow automated linking. As the document has been through many stages of preparation, how many different versions need to be separately recorded? Each of these requires the exercise of functional granularity: the provision of a way (or ways) of identifying parts and versions whenever the practical need arises.

The application of functional granularity depends on a huge range of factors, including the type of resource, its location in time and place, its precise com-

¹⁰³ See: ISBN (1992).

¹⁰⁴ See: NISO (2000).

position and condition, the uses to which it is or may be put, its volatility, its process of creation, and the identity of the party identifying it. The implication of this is that a resource may have any number of identifiers. The same entity may be subjected to functional granularity across a range of views. The basic “elements” of a resource may be entirely different according to your purpose. Stuff may be analysed, for example, in terms of molecular entities (chemistry), particles such as electrons, quarks or superstrings (physics), spatial co-ordinates (geography), biological functions (biology, medicine), genres of expression (creations), price categories (commerce), and so on. In the digital environment, stuff can be relatively easily managed at extreme levels of granularity as minute as a single bit. Each of these process will apply identifiers of different types at different levels of (functional) granularity in different “dimensions”; these may need to be reconciled to one another at a point of higher granularity.

Functional granularity does not propose that every possible part and version is identified: only that the means exists to identify any possible part or version when the occasion arises. Identification is not the same as mark-up, though if a section is distinguishable by some mark-up coding it will be subsequently easier to specify it as separately identified.

X.2 Conflicting Views of Granularity: Difference within Sameness

What is “the same thing” for one user, purpose, or context will be “two different things” for another. The two users may have different purposes in mind when they ask “are X and Y the same?”; and as we have seen, this question is implicitly “are X and Y the same for the purpose of...?” Failure to comprehend these different views (purposes) across a supply chain results in considerable friction. Some practical examples will illustrate this. For clarity, I refer in each case to two different users — the party who sees “the same thing” as X and the party who sees “two different things” as Y.

There has been much discussion (as yet not fully resolved) of this in the context of eBooks¹⁰⁵: publisher X wishes to use one identifier (the ISBN) to refer to all technical formats of an eBook, since they are all “the same book”; yet supplier Y needs to distinguish different formats (a customer ordering one format wants that and no other). Some publishers have in fact suggested using the ISBN with some form of qualifier (or parameter) to do this; the International ISBN agency prefers to recommend different ISBNs for each format¹⁰⁶. These are the two general approaches to recognising difference within sameness, each of which may be valid in some circumstances: a “*single identifier with qualifier*” or “*create new multiple fixed identifiers*”.

The “single identifier with qualifier” approach is used in solving the “appropriate copy” problem in one application with DOIs¹⁰⁷. The generalised case is that since an identifier is normally that of a class (an abstraction), it is assumed that

¹⁰⁵ See: Anderson Consulting (2000).

¹⁰⁶ See: ISBN (2002).

¹⁰⁷ See: Beit-Arie (2001).

each member of the class is equivalent; but in reality this may not be so in all contexts, and there are many instances when more than one legitimate copy is available, and some copies are not available, due to the context of the request. In the appropriate copy example, publisher X allocates one identifier to an article; library user Y finds that because of local loading, aggregator databases, paper copies or mirror copies, she needs to distinguish copy one from another; in each of these cases, the address to which the identifier given by X should appropriately resolve depends on the location or affiliation (in general, the context) of the user Y who is making the resolution request. To solve this problem it makes sense to contextualise the use of the identifier by some tool such as OpenURL. A full analysis of any transaction, in the further work done using indecs for MPEG¹⁰⁸, shows that ultimately all transactions are contextual and can be expressed as an event or a situation; and a full analysis of the use of identifiers will show that ultimately of course they are all used in some context.

The “create new multiple fixed identifiers” approach is shown in the emergence of the ISTC. New identifiers may be needed and require the creation of a new namespace if the namespace currently being used cannot satisfactorily include a new type of entity without disrupting the existing business. A good example is the identification of textual abstractions and the identification of their manifestations (books): ISBNs are in widespread use for identifying (separately) each different edition of e.g. Cervantes’ *Don Quixote*. These are different (if customer Y orders the leather bound limited edition with illustrations by Dali, he is unlikely to be happy to receive the \$1.50 Worlds Classics paperback edition). Yet authors agencies, rights organisations, and librarians X may all be interested in the general work and not concerned with specific editions for some purposes (a library reader wishing to find a copy of the work, for example). This led to the development (with the full collaboration of the ISBN agency) of a new identifier, the ISTC, which can be used to identify this entity (the textual abstraction)¹⁰⁹. This example also usefully shows that it is not always the smaller granularity entities which the driver for the creation of new identifiers: in this case, a new identifier is required which may be related to “supersets” of ISBNs.

These two ways of dealing with “difference within sameness” are not always clear black-and white alternatives, and once again functional granularity will be the arbiter of which to use in which cases: is there a need to agree on a separate identification scheme (a new namespace), or can we live with the difference being defined by qualification after the identification step at a local level, which is not likely to be widely used across a supply chain? If the entities being finely differentiated are the object of commercial transactions across multiple partners, or are likely to be stored and used in communication to identify precisely the differentiated entity (rather than the unqualified entity), then I believe the separate new identifiers approach is likely to be optimal in the long term.

In each solution, the same logic applies: whether we refer to them as “a qualified identifier with two different qualifiers” or “two identifiers which have a relation”

¹⁰⁸ See: MPEG-21 RDD (2003).

¹⁰⁹ See: ISTC.

is semantics: “ISBN 1234” and “ISBN1234—as qualified—Z” are separate strings. They denote different entities, they must do otherwise there wouldn’t be a need for two strings. It may well be that party X only needs the first, but if party Y has a need to deal with all these different transformations generated by X at a business level and needs to know the various sub “qualified” identifiers, then Y is going to end up having to store the [qualified] identifiers and treat them as static separate strings, i.e. separate identifiers — probably in a separate database because the particular numbering system X has used isn’t sufficiently granular for Y’s needs.

If entities need at some point to be differentiated for long-term purposes (which typically they do in any DRM chain for e.g. audit etc.), then inescapably someone somewhere will be managing multiple identifiers [strings] with multiple metadata [as there are multiple entities] that have a defined relationship. This need not be a concern if that management is in an isolated internal database, but increasingly such data is becoming exposed to interoperability, the heart of DRM. Wherever this happens, this is easier to do by treating all differentiable entities as having fixed identifiers — persistent opaque strings with associated data — rather than some as derived by qualification. This allows a common mechanism for persistence, registration, and interoperability. There are many related identifier labels (namespaces) and no one can deal with all possible needs — this is why ISTC had to be added on top of ISBN, rather than overloading one system and asking it do two fundamentally opposing jobs; an identifier system or framework which can contain all these, such as DOI, is making more and more sense.

XI Intelligence in Identifiers

A dumb identifier is an opaque identifier string that serves solely as unique label and has no other inherent or implied meaning (synonyms: simple or insignificant identifier). An example is a manufacturing sequence number; a consortium of manufacturers may use this as an interoperable identifier by preceding each string with some means to guarantee uniqueness across originators. In text publishing, an early example was the PII (Publisher Item Identifier) [PII], simply a sequence number from an individual publisher (and incidentally a precursor of the ISTC; most PIIs are now used in the form of DOIs through the CrossRef implementation¹¹⁰).

An intelligent identifier is a string that has at least some segment capable of ready interpretation outside the identifier scheme to derive meaningful information (synonyms: compound or significant identifier). Intelligent identifiers which carry some information in their structure relating to the entity they identify, such as a format, date or producer code, are of some value in particular circumstances, but problems of ambiguity or volatility often render much of this apparent “intelligence” unreliable. A manufacturing sequence number that explicitly included as its opening string the year of manufacture would contain

¹¹⁰ CrossRef — Web Site: <http://www.crossref.org>.

such intelligence. The SICI (Serial Item and Contribution Identifier)¹¹¹ contains substrings denoting elements such as date of publication, page number, etc. Intelligence is the insertion into the name syntax for one namespace of a string which has applicability in another namespace: it therefore creates a hard-wired link between the two entities in the two namespaces: i.e., metadata. Hard wiring is appropriate only if the relationship will never need to change, which is not always easy to guarantee (as the year 2000 problem amply demonstrated).

“Affordance” is the ability to enable construction of a unique identifier from examination of the physical manifestation (or some metadata record of it), rather than by reference to a central database of identifiers¹¹². Affordance is therefore a counterpoint to the concept of intelligence: intelligence implies ability to derive, some element of metadata about the object, from the identifier; affordance implies the ability to derive the identifier from the object or metadata. Another term for this is computability: given the object instance, the identifier for a namespace may be computed. The SICI scheme allows a SICI code to be created by algorithm from known citations; while this could be done manually, it can be automated by algorithms¹¹³. This enables a user to retrieve citation records from various databases, and subsequently create the SICI code that could then be used to search more efficiently across multiple text databases to find the actual article. Given the variation and performance of search capabilities across multiple systems, an algorithmic key is more likely to find the document than a reformatted version of the initial query or bibliographic citation textual elements. For the SICI or other such access keys to be highly successful, more standardization of bibliographic citation data elements is needed; however, it seems to hold promise for locating a bibliographically denoted work from numerous different online resources and legacy systems.

XII Aids to Identifier Use: Readability and Check Digits

Readability refers to the design of identifier syntax in such a way as to aid interpretation by human inspection in an application. The design of the Internet domain name system is a clear example where simple IP addresses (numerical values) are associated with more readable or memorable strings (such as `www.ibm.com`); the price to be paid for this is literal, in that certain memorable or readable strings become much more valuable than others in a commercial context, although the underlying numbers appear to be of identical value. Readability can be assisted even in numeric, dumb, schemes: an example is the Publisher Item Identifier (PII) which consists of seventeen alphanumeric characters in a single string (e.g. `S1384107697000225`); for readability when the PII is printed slashes, space and parentheses are added where necessary, to ease the reading of

¹¹¹ See: NISO (1996).

¹¹² See: Green, Bide.

¹¹³ See: Paskin (1999).

the code and divide it into segments each with a defined origin though not meaning (e.g. S1384-1076 (97) 00022-5). These additional elements are stripped out for machine readable use and/or reinstated on printing and do not form part of a machine-readable string or check-digit algorithm. Readability is important if an identifier will be entered by keyboard rather than automatically. Readability is not necessarily synonymous with intelligence (the DNS example uses intelligence, the PII example does not), though where an intelligent number is used readability will be enhanced by visually parsing into the component intelligent elements. Readability may also help in some limited cases of error correction (e.g. recognising that a string 3002 representing a year should really be 2002).

Identifier labels may contain a check digit: usually the last in the sequence within an identifier string, algorithmically derived from the preceding digits, rather than being part of the identifier itself. The aim is to ensure that if one digit is incorrectly transcribed, the check digit will change as an alerting mechanism, and that if two digits are incorrectly transcribed, the chance of their combined effect on the check digit cancelling each other out is minimised. Recalculation of the check digit from the body of the number, followed by comparison with the stated check digit, can be performed algorithmically at key points in processing. Note that this provides error detection, but not error correction. In a typical check digit algorithm, each digit is assigned a different weighting factor (ideally a prime number). Digits and their corresponding factors are individually multiplied and summed, the resulting sum divided by a prime modulus number, leaving a remainder being the check digit; using prime numbers minimises the chances of internal cancellation. Check digits occur in for example ISBN and ISSN numbers and in other contexts, e.g. bank account numbers; ISO has a recommended standard for check digits¹¹⁴. Check digits are typically of importance in an entry step (where identifiers have to be manually transcribed as input) and less important in a transmission step where error correction protocols such as packets (TCP/IP) are already in place, although their original introduction was to ensure consistency in both types of activity.

Internet systems have error correction in the transmission protocol, but not on entry: URLs (URIs) do not contain check digits. This may lead to the assumption that check digits are of less importance, in an Internet-enabled world, than had been assumed in earlier automation phases. Whether or not this is true depends to some extent on the consequences of an error slipping through: whether inputting an incorrect identifier generates an error message, or simply locates the wrong object. A message may be transmitted correctly, but contain incorrect initial input: e.g. omitting check digits in bank account numbers would not provide adequate error protection for most users.

¹¹⁴ International Standard Data processing — Check character systems — ISO 7064:1983¹¹⁵.

¹¹⁵ Available at: <http://www.iso.ch/iso/en>.

XII.1 Resolution

Resolution is key to creating actionable identifiers from simple labels in a digital network, through implemented schemes. Resolution is a process in which an identifier is the input (a request) to a network service to receive in return a specific output of one or more pieces of current information related to the identified entity: e.g. a location (such as URL) where the object can be found. The technology supporting this capability is a *resolver*. In the case of the Domain Name System (DNS), as an example, the resolution is from domain name, e.g., `www.doi.org`, to a single IP address, e.g., `132.151.1.146`, which is then used to communicate with that Internet host. In the Handle System¹¹⁶, a well-designed and scalable resolution system designed by one of the originators of TCP/IP, the resolution is from a “Handle” to one or more pieces of typed data: e.g. URLs representing instances of the object, or services, or one or more items of metadata. Resolution can be considered as a mechanism for declaring a relationship between two data entities; an item of metadata is a relationship that someone claims exists between two entities: therefore, metadata relationships between entities may be articulated and automated by resolution.

In computer science terms, resolution is “adding a level of indirection” (sometimes called redirection): manipulating data via its address. Indirection is a powerful and general programming technique of processing data by maintaining a pointer to the current item and incrementing it to point to the next item, such as a new value. Providing that the performance issues of adding this extra communication step can be overcome, indirection is a very useful way of separating one into a relationship of two entities, which may then be separately managed — e.g. a name and a location. This then provides a mechanism for managing persistence of the name even if the location varies.

The concept of the URN (Uniform Resource Name) was introduced into the Internet to allow indirection, such as “N2L” (URN to URL) resolution. One of the earliest applications for DRM was the DOI for simple, single point resolution. Each DOI has at minimum a single URL to which it will resolve. This allows the location of an entity to be changed while maintaining the name of the entity as an actionable identifier. DOI is not alone in providing a solution to this problem. Other applications, for example PURLs (Persistent URLs), can provide this simple level of resolution. It has been argued — though increasingly this is a lost cause — that URLs can (in theory) themselves be used as a persistent identifier — that their use as a transient identifier is a social, not a technological, problem. However, this lack of persistence of the URL is only the first of many challenges that the DOI System was designed to manage.

¹¹⁶ The Handle System — <http://www.handle.net/>.

Handle RFCs — <http://www.handle.net/documentation.html>.

See: Sun, Lannom (2002); Sun, Reilly, Lannom (2002); Sun, Reilly, Lannom, Petrone (2002)

XIII Multiple Resolution

An identifier is a name for an entity; in the network environment, there may be many identical copies (“instances”) of the same piece of content. A single identifier may be used to manage the existence of multiple “instances”, or multiple metadata relationships, or multiple services, if the resolution step can offer linkage not simply from one identifier to a single piece of data (e.g. a URL), but to multiple data. The Handle System is such a multiple resolution technology (a URI and in conformance with URN, as discussed below). The need for multiple resolution if one is to construct any complexity is obvious if one envisages the resolution process as a set of connections between points in a logical space: univalent linkage (single resolution) offers very limited construction possibilities (simple chains); polyvalent linkage (multiple resolution) offers unlimited branching constructions.

The Handle System is used in e.g. the DOI, the D-Space project¹¹⁷ and other systems¹¹⁸. Uniquely, by using the Handle System in combination with the indecs approach to metadata, the DOI system provides a full framework for identifiers to be articulated by means of resolution and interoperable metadata. The DOI System is also designed to manage much more complex DRM-related services than resolving to multiple instances of the same piece of content, such as accessing metadata about the entity that the DOI identifies. At its simplest, the user may be provided with a list from which to make a manual choice. However, manual choices are not a scalable solution for an increasingly complex and automated environment. The DOI will increasingly depend on automation of “service requests”, through which users (and, more importantly, users’ application software) can be passed seamlessly from a DOI to the specific service that they require.

XIV Persistence

Critically for DRM, even if ownership of the entity or the rights in the entity change, the identification of that entity should not change. The responsibility for managing the identifier may change, but not the identifier itself.

The lack of persistence in identification of entities on the Internet is a commonplace. Even the most inexperienced of users of the World Wide Web rapidly becomes familiar with the “Error 404” message that means that a specified Web address cannot be found — the URL for that web page cannot be resolved. Resolution offers a mechanism to assist, by assigning names rather than locations. But persistence is ultimately guaranteed by social infrastructure (policy); persistence is fundamentally due to people, and technology can assist but not guarantee.

¹¹⁷ DSpace Web Site: <http://www.dspace.org>.

¹¹⁸ Applications of the Handle System: <http://www.handle.net/apps.html>.

A URI should persistently identify a resource. A DOI (a URI with specific application in intellectual property plus added features) identifies a specific intellectual property entity, which may or may not be an Internet-accessible file, and ensures persistence through policy; a URL identifies a specific address on the Internet. These applications of identification are completely different. One identifies an entity; the other identifies a location (where a specific entity may or may not be found). The analogy is with the ISBN (which identifies the book) and the shelf-mark (which identifies the place where the book is to be found). When the location changes, the shelf mark changes — but the ISBN does not.

Identifiers must persist in the face of legitimate change. There are legitimate, desirable, and unavoidable reasons for changing organisation names, domains etc. One aim of naming entities/resources is to avoid tying an entity name to a domain name, or any other piece of variable metadata (a problem encountered in recent domain names/trademarks disputes). The entity can be persistently named as a first class object irrespective of its location, owner, licensee, etc. Distinguishing names from locations is essential for E-commerce. It is trivially true that “all names are locations” (in a namespace), but practically, most people worry about spaces like URLs, and that’s the wrong level. Naming entities as first class objects, rather than locations, enables better management of multiple instances of an object, for example.

Persistence is something we are familiar with in the physical world: ISBNs for out of print books can still be useful. Persistent identification alone is a good enough reason to adopt identifiers such as DOI which provide a means by which potential customers can find your digital offering even if a “broken link” URL of a retailer or other intermediary intervenes.

Technology can help with persistence. For example using DOIs, only one central record, which is under the control of the assigner, needs to be changed in order to ensure that all existing DOIs which are “out there” in other documents can still resolve correctly: a redirection resolution step enables management in the redirection directory, thereby ensuring that one change can be picked up by many users, even if they are unaware of the change. But to manage the data in the directory takes effort, time, incentive, etc. — either you do that locally (using tools such as PURL, managing a service yourself) or as a global service (the DOI being such a service for intellectual property entities). In the case of DOI management of data is a service role (and hence also business activity) for registration agencies, an approach used in other activities like bar codes and ISBNs. People aren’t free, so there’s a cost to this, and just like the physical bar code system, the DOI aims to be a self-funding operation. DOIs won’t be appropriate for many things, and some people won’t feel this people cost merits the reward, but DOIs (or any other system which offer similar functionality) are a viable solution for content management of intellectual property on a large scale.

DOI is an implementation of URN (Uniform Resource Names) and URI (Universal Resource Identifier) concepts, and can be formalized within these frame-

works. The aim of each is to allow persistence of naming irrespective of other characteristics.

In addition to persistence of the identifier, a fully operational service such as DOI has to consider also persistence of the resolution technology, persistence of the identified object (archiving and preservation); and stability and invariance of the associated metadata. These topics are beyond the scope of the present article and interested readers are referred to other discussions¹¹⁹.

XV Internet Specifications for Identifiers

Ideally, to ensure efficient use across many DRM applications we should follow the *principle of application independence*: metadata structures should be independent of any specific technical expression. Identifier and metadata systems whose development is shaped by technical rather than semantic constraints will be less than optimal, but technological differences must be resolved at the point of interoperability, since they cannot be wholly anticipated at source; so we cannot always follow this principle in full. Internet usage of identifiers is of particular significance in DRM.

XV.1 Uniform Resource Identification Specifications

URN (Uniform Resource Name) and URI (Uniform Resource Identifier) are specification schemes for persistent identifiers of resources in the Internet. Existing identifiers such as ISBN, ISMN, DOI etc. may be registered as URI and URN schemes, to enable implementations to make use of the technical specification. URIs and URNs should therefore be considered as a “framework” for enabling identifiers to work in an internet environment, rather than as a competing system of identification to existing schemes such as ISO identifiers (as explained above, ISBNs are labels, and URI/URN are specifications for using those labels in a digital context.)

In order to make use of such specifications, an implementation mechanism must be put into place. It is important to distinguish two issues:

- The Internet specifications of “what is” a URN and a URI: these differ slightly from each other (see below);
- What this means for practical implementation: irrespective of internet specifications, to make use of persistent identification schemes in useful ways will usually require more than a simple technical implementation. Especially, policy and governance issues (such as scope, authority to issue), and control of assigned metadata (quality control, interoperability considerations, etc.) will be important components in adding value in practical implementations (an “implemented identifier system” as described above).

Definitions and of the URN and URI concept are spread across a number of documents; the specifications are also continuing to evolve. “Naming and Addressing:

¹¹⁹ See: DOI (2003): chap. 7.

URIs, URLs, etc.”¹²⁰ provides an overview of W3C (World Wide Web consortium) materials related to Addressing. Recently (November 2002) the W3C has proposed a further “URI Activity”¹²¹ to deal with remaining issues of URI and URN definition, documentation, and reconciliation. The URN concept was originally driven by the IETF; the URI concept by the W3C.

URI, Uniform Resource Identifier, is defined as “the generic set of all names/addresses that are short strings that refer to resources”. In some publications from W3C, URI is also defined as “Universal Resource Identifier”. A URI may be a pure name or de-referenced by any service; in the latter case, the namespace provides its own mechanism (“bootstrapping”). On its own, any URI specification is just a specification: it requires code distribution for any implementation. URI schemes are only intended to “address information spaces that are globally useful”¹²². URIs are not intended to rely on any additional network services. A software client either knows what to do with, e.g., ftp, or it does not: this is the key difference with the URN specification.

URN, Uniform Resource Name, is defined according to W3C in two ways: (1) as “an URI that has an institutional commitment to persistence, availability, etc.;

(2) as “a particular scheme, urn:, specified by RFC2141 and related documents, intended to serve as persistent, location-independent, resource identifiers.” Thirteen RFCs specify URN syntax, services, namespace registration process and technical implementation of URN resolution in the present Internet¹²³. URN architecture¹²⁴ assumes an additional network service that would allow a client to deal with a previously unknown URN type, e.g. *urn:isbn*. Specifically, a DNS-based middle layer (RDS) is used to find the specific service appropriate to the given URN scheme. URN resolutions are then delegated to that scheme-specific resolution service. The original RDS mechanism proposed was NAPTR (Name Authority Pointer); more recently a variant of this, DDDS (Dynamic Delegation Discovery System) has been proposed. These are proposed DNS extensions that would use DNS to provide a regular expression for the namespace, e.g., turn *urn:isbn:1234567890123* into [http:// isbn.org/1234567890123](http://isbn.org/1234567890123). These have not so far been widely used in a production sense: there are no practical implementations of large scale. There may be identifier strings being laid down as specifications (fifteen URN namespaces have already been registered, including several ISO identifiers such as ISSN and ISBN, and National Bibliography Numbers, NBNs), e.g., *urn:isbn:123456789*, but at this point there is no apparent advantage to that over the simpler *isbn:12345678*. In neither case is there a readily available well known global resolution service. Implementations (most are in libraries and are based on NBNs¹²⁵) rely on local distribution of specific plug-ins and know-how.

¹²⁰ W3C: “Naming and Addressing: URIs, URLs, etc”. Available at: <http://www.w3.org/Addressing/#19991>.

¹²¹ See: W3C (2001).

¹²² See: Palmer (2001).

¹²³ URI.net web site: <http://www.uri.net/>.

¹²⁴ See: URN (1997).

The DOI System implements the URI/URN notions to enable identifiers to be global persistent and actionable object names, with the added aim of doing this in a coherent way across a wide range of media types and identifier schemes. Name resolution is currently by two separate methods to reference DOIs on the Internet: as URIs (`doi:10.123/456`) and as URLs (`http://dx.doi.org/10.123/456`). Each string can stand on its own, as a pure unique name, or it can be resolved using some network service. Resolution of the URI form would require software not yet commonly found on users' desktops (but which can readily be supplied by means of plug-ins such as for the Handle System¹²⁶). Resolution of the URL form requires a proxy or gateway service out on the network. Existing identifier schemes may use DOIs or adopt their own individual resolution scheme: if these individual schemes are successfully and widely deployed the identifier would then be usable as a persistent name for that namespace alone.

XV.2 Persistent URLs (purls)

A PURL is a Persistent Uniform Resource Locator¹²⁷. Functionally, a PURL is a URL. However, instead of pointing directly to the location of an Internet resource, a PURL points to an intermediate resolution service. The PURL resolution service associates the PURL with the actual URL and returns that URL to the client. The client can then complete the URL transaction in the normal fashion. In Web parlance, this is a standard HTTP redirect. PURL was devised by OCLC's Office of Research after participating in the IETF URI work. There is nothing incompatible between PURLs and the ongoing URN (Uniform Resource Name) work; PURLs satisfy many of the requirements of URNs using currently deployed technologies and can be transitioned smoothly into a URN architecture once it is deployed.

PURLs are all http based. This is both their strength and their weakness. When you send a PURL to a PURL server, you are sending a special URL to a web server via http, and the web server will send back a perfectly typical web server answer — all http. The difference is that there is a special PURL server or module linked to that web server that inspects the URL, looks at a table to see what it means today, and returns that. It is one level of indirection, just like a single value DOI or Handle, but it is all contained within a single server and that single server is permanently attached to a specific domain name: PURL servers don't know about each other. In some ways it is no different from the way DOI uses a Handle proxy, `dx.doi.org`, which re-interprets DOI Handle queries into http (if DOI were never going to go beyond the proxy server approach and never make use of the multiple resolutions and data types, PURL would be a comparable technological component to the DOI's chosen Handle protocol. There are ways in which one might imagine PURLs being developed to provide an approximation towards multiple resolutions and multiple data types. Content negotiation has

¹²⁵ See: IETF (2001).

¹²⁶ "Handle System plug in". Available at <http://www.handle.net/resolver/index.html>.

¹²⁷ Persistent Uniform Resource Locator Web Site: <http://www.purl.org>.

always been in http, but like most W3C considerations is oriented at attributes of the document in hand. The more you push this, from document centric things like “give this to me in German” to more “attributes” like “tell me about rights”, the more tenuous the approach would become.

As PURLs are http, they are designed to be used only in the web: this may not be an obvious problem at present, but the development of many mobile and other platform technologies means that not everything that happens on the internet from this point forward will necessarily be an extension of the www protocols; nor will DRM solutions which are based on web-only techniques prove satisfactory to the content industry (URN and URIs by contrast can be implemented with other protocols). PURLs have been widely available for several years but are not widely implemented in commercial settings and do not provide a sufficiently sophisticated infrastructure for identification in relation to DRM (though to be clear, no one would claim that PURLs provide such a comprehensive facility; they are a useful tool for simple local persistence management).

XVI DRM Identifier Implementations Require Metadata

In assigning an identifier to a single digital entity it is necessary to also provide some defining attributes if that identifier is to be widely useful. Identifiers are simply names: names that follow a strict convention and are unique if properly applied. Unique identifiers are particularly valuable in machine-mediated commercial environments, where unambiguous identification is crucial. Some identifiers tell you something about the thing that they identify — for example, since “ISBN” is the acronym of “International Standard Book Number”, the identifier “ISBN 1-900512-44-0” can reasonably safely be assumed to identify a book (always assuming that ISBN rules have been correctly followed). However, to find out which book it identifies, it is necessary to consult metadata — the identifier links the metadata with the entity it identifies and with other metadata about the same entity. Metadata is an integral part of making the identifier useful. Some of this metadata may be held in private systems (the publisher’s warehouse system, for example) but some of it is more widely available (e.g., Books in Print).

If a digital identifier simply offers a system providing persistent single point location on the Internet (e.g. PURL), then metadata is not be essential to its function. However, for DRM uses, the identifier system must provide the basis for a full range of services relating to intellectual property in the network environment: metadata becomes an essential component. It is easiest to discuss this concept by considering a specific example, the DOI, which has been designed specifically with DRM uses in mind. The DOI can identify any kind of intellectual property entity, and because it is by design an “opaque string”, the user can tell nothing about what it identifies from just looking at the DOI: the user can access and inspect metadata related to the DOI, since the entity it identifies may not itself be open to direct inspection — it may be an abstract “work”

or a performance. Metadata is needed because a number alone does not impart anything useful (like a telephone number without an attached name). To use the identifier we need some additional data, for example:

- what is the creation that is identified?
- does it have another identifier I might know (e.g., an ISBN?)
- does it have a name (title)?
- who are the parties responsible for its creation or publication?
- what sort of thing is it? (abstract, physical, digital or spatio-temporal),
- what is its mode? (visual, audio, etc.)
- does it belong to a particular application type (e.g., article linking)?

We cannot list “all metadata” associated with an entity (by definition impossible) but a limited “kernel”, applicable to all DOIs and meeting these requirements, is the basis for extensions to specific purposes (Application Profiles), using the Handle system ability of multiple resolution as a tool¹²⁸. Using the principles of interoperability defined by indecs, these Application Profiles can be defined in existing metadata schemes, where that makes sense for a particular user community (ONIX, SCORM, SMPTE, DC). A DOI application will use a particular set of metadata: we call this an Application Profile. If metadata is to be commonly accessible by applications, common format(s)/schemas must be used and registered. This implies a standard vocabulary or data dictionary for mappings to/from both the kernel and the wider application sets. Metadata permits both recognition of the entity that is identified by a DOI and its unambiguous specification; it also allows for the interaction between the entity and other entities in the network (and with metadata about those entities).

XVII Well-formed Metadata; The <indecs> Framework

The analysis of the <indecs> project on interoperability of data in e-commerce systems¹²⁹ clarified the requirement for unambiguous “well formed” metadata. This does not propose that all metadata for intellectual property has to be managed in a single metadata scheme. It does though propose that all such metadata needs to be “well formed”; this will allow metadata developed in conformance to different schemes to interact or “interoperate” unambiguously. Without that interaction, different metadata schemes risk becoming the “trade barriers” of the future. There are only two types of metadata that can be regarded as well formed:

- Free-form labels: the names by which things are called (of which “titles” are a subset). These are by their nature uncontrolled and broadly uncontrollable. Identifiers (in the sense of section 5.1) are a specialized type of label, created according to rules, but names nevertheless. The fact that they are created in accordance with a prescribed syntax makes them less prone to ambiguity

¹²⁸ See: DOI (2003): chap. 5.

¹²⁹ <indecs> Web Site: <http://www.indecs.org>.

than other types of label and therefore more readily machine–interpretable than completely free–form labels.

- Metadata drawn from a controlled vocabulary of values, which are supported by a data dictionary in which those values are concisely defined. This means that the values in one metadata scheme (or in one “namespace”) can be mapped to those in another scheme; this mapping may not be exact — where two definitions in one scheme both overlap with (but are not wholly contained within) a single definition in another, for example. However, the use of a data dictionary avoids the sort of ambiguity that is inherent in natural language, where the same word may have very different meanings dependent on its context. Where precision of meaning is essential, human beings can clarify definition through a process of dialogue. This is not generally the case with computers.

The mapping between different metadata schemes may be more or less exact. It may also involve considerable loss of information or no loss of information at all. It is obviously advantageous to achieve as close a mapping as is possible; this is most easily achieved between schemes that share a common high–level data model. The <indecs> data model underlies all DOI metadata. The same analysis underlies ONIX International¹³⁰, rapidly becoming widely accepted as the metadata dictionary for the publishing industry internationally. Similar developments are now occurring in other media sectors (e.g. the adoption of indecs by MPEG-21).

Fundamental principles defined within the indecs project and used within DOI are:

- *Unique identification*: every entity needs to be uniquely identified within an identified namespace;
- *Functional granularity*: it should be possible to identify an entity when there is a reason to distinguish it;
- *Designated authority*: the author of metadata must be securely identified;
- *Appropriate access*: everyone requires access to the metadata, on which they depend, and privacy and confidentiality for their own metadata from those who are not dependent on it.

The <indecs> data model was devised to cover all types of intellectual property (“creations” in <indecs> terminology). It is an open model, which is designed to be extensible to fit the precise needs of specific communities of interest. It was also designed to be readily extensible into the field of rights management metadata, the data that is essential for the management of all e–commerce in intellectual property. The <indecs> analysis asserts that it is essential for the dynamic data necessary for the management of rights to be built on a foundation of the rather more static data that identifies and describes the intellectual property, and that these two layers of metadata can easily interoperate with one another. <indecs> was a time–limited project, which finished its work early in 2000. Its output is highly regarded and its analysis has been adopted in a

¹³⁰ See: EDItEUR.

number of different implementations. The work has since been developed and further elaborated, and forms the basis for the ISO MPEG-21 rights data dictionary discussed below.

Simple metadata solutions, the most notable being the Dublin Core¹³¹ developed as a means of encouraging resource discovery on the Web by having content creators declare any of a small core of 15 elements to their creations, do not follow these principles. The original aim of Dublin Core has been very much superseded by the remarkably effective “resource discovery” search engines such as Google, leaving a large amount of effort on metadata in search of a new area of application, and it unfortunately has been too tempting to divert this original effort into other applications which require considerably more complexity than resource discovery. “The Dublin Core, while far from perfect from an engineering perspective, is an acceptable standard for such simple metadata [but] efforts to introduce complexity into Dublin Core are misguided”¹³².

Indecs provides an ontology (an explicit formal specification of how to represent the objects, concepts and other entities that are assumed to exist in some area of interest and the relationships that hold among them) for talking about Intellectual Property transactions and so will inform the creation of, or simply provide, the metadata terms for articulating practical DRM applications.

Without an ontology and structured framework, metadata terms and classifications become ultimately useless for anything other than the purpose the deviser had in mind, recalling the famous parable of Jorge Luis Borges¹³³: “*These ambiguities, redundancies, and deficiencies recall those attributed by Dr. Franz Kuhn to a certain Chinese encyclopaedia entitled Celestial Emporium of Benevolent Knowledge. On those remote pages it is written that animals are divided into (a) those that belong to the Emperor, (b) embalmed ones, (c) those that are trained, (d) suckling pigs, (e) mermaids, (f) fabulous ones, (g) stray dogs, (h) those that are included in this classification, (i) those that tremble as if they were mad, (j) innumerable ones, (k) those drawn with a very fine camel’s hair brush, (l) others, (m) those that have just broken a flower vase, (n) those that resemble flies from a distance*” (“The Analytical Language of John Wilkins”).

The indecs definition of metadata (“an item of metadata is a relationship that someone claims to exist between two entities”) provides a concise paraphrase of much of the <indecs> framework. It stresses the significance of relationships, which lie at the heart of the <indecs> analysis. It underlines the importance of unique identification of all entities (since otherwise expressing relationships between them is of little practical utility). finally, it raises the question of authority: the identification of the person making the claim is as significant as the identification of any other entity.

¹³¹ Dublin Core Metadata Initiative — <http://dublincore.org/>.

¹³² See: Lagoze (2001).

¹³³ See: Borges (1999).

XVIII Tools for Expressing Metadata Elements

The indecs framework is an abstract ontology, independent of medium and technology. Techniques are being developed which are appropriate for expressing such ontologies (structured data) on the web, notably RDF and TopicMaps. In the long term, the vision of “the semantic web” will require such ontologies and means of expressing them.

RDF, the Resource Description Framework¹³⁴, provides “a lightweight ontology system to support the exchange of knowledge on the Web” (the weasel word here is “lightweight” — for serious DRM applications, a lightweight approach may or may not be insufficient) — RDF is essentially a way of representing ontologies as attributes and relationships using XML.

The TopicMaps specification¹³⁵ provides a model and grammar for representing the structure of information resources used to define topics, and the associations (relationships) between topics, again using XML. Names, resources, and relationships are said to be characteristics of abstract topics, which have defined name, resource, and relationship. One or more interrelated documents employing this grammar is called a “topic map”.

The ISO 11179¹³⁶ standard for data elements provides a means of specifying basic aspects of data element composition, including metadata. The standard applies to the formulation of data element representations and meaning as shared among people and machines; it does not apply to the physical representation of data as bits and bytes at the machine level; nor does it speak to semantic mappings (ontologies), but if DRM identifiers and metadata are able to adopt ISO 11179 principles without disadvantage, there are obvious benefits in terms of making data widely available in a readily understood form. An ISO 11179 data element is composed of three parts:

- an object class: a set of entities
- a property: a peculiarity common to all members of an object class;
- a representation, describing how the data are represented, i.e. the combination of a value domain, datatype, and, if necessary, a unit of measure or a character set.

The combination of an object class and a property is called a data element concept (DEC). ISO/IEC 11179 provides procedures and techniques for associating data element concepts and data elements with classification schemes for object classes, properties and representations and related tools such as the assignment of numerical identifiers that have no inherent meanings to humans, icons, etc.

Once a set of elements is precisely defined for a schema and readily available in some format such as XML, the schema can be used in interoperable applications.

¹³⁴ W3C Web site: Resource Description Framework: <http://www.w3.org/RDF/>.

¹³⁵ TopicMaps.org Web Site: <http://www.topicmaps.org/>.

¹³⁶ See: Metadata Registries.

Commercial tools such as Adobe's Extensible Metadata Platform (XMP) are now coming on stream¹³⁷ and promise to take the concepts of structured metadata and XML and provide a widespread means of applying them, though it remains to be seen how successful these become.

XIX Interoperability

In the <indec> framework, interoperability means *enabling information that originates in one context to be used in another in ways that are as highly automated as possible*. Commerce does not necessarily mean the exchange of money: any environment where creations are made or used employing electronic means is encompassed by commerce in this sense.

The information that needs to interoperate here is metadata: data of all kinds relating to creations, the parties who make and use them, and the transactions that support such use. The problems to be overcome are often as simple as the fact that a term such as "publisher" has a quite different meaning in two different environments which now need to exchange metadata; they are also as complex as the fact that a single creation may contain a hundred distinct pieces of intellectual property, the rights of which are owned or controlled by many different people for different purposes, places and times. Changes in the status or control of these rights, recorded in different and unconnected systems, will need to be capable of being communicated automatically in many different ways.

XIX.1 Types of Interoperability

Interoperability in e-commerce has many different dimensions. As traditional sectors and business models break down, organisations increasingly face the need to combine or access information that arrives in a variety of forms and that comes from a variety of sources. The creator of metadata about a piece of intellectual property will want to be sure that the accuracy and effectiveness of the information he creates (often at substantial cost) can survive intact as it negotiates a range of barriers. Automated DRM needs to support interoperability of at least six different types:

- Across media (such as books, serials, audio, audiovisual, software, abstract works, visual material).
- Across functions (such as cataloguing, discovery, workflow and rights management).
- Across levels of metadata (from simple to complex).
- Across linguistic and semantic barriers.
- Across territorial barriers
- Across technology platforms.

A good e-commerce metadata system therefore needs to be multimedia, multi-functional, multi-level, multilingual, multinational and multi-platform. Such an approach may be said to be well-formed.

¹³⁷ See: Rosenblatt (2002).

The failure of interoperability in each of these dimensions can be seen as trade barriers to e-commerce interoperability. These barriers are not all yet generally critical, only because the volume of e-commerce traffic in intellectual property is relatively modest: yet we are now seeing an unprecedented explosion in the development of intellectual property metadata schemas. Listed alphabetically below are just some of the major initiatives where substantial metadata vocabularies, models, databases and/or interchange formats are currently being developed or deployed, showing the communities in which they currently operate or from which they were originated:

ABC ¹³⁸	(general ontology model)
CIDOC ¹³⁹	(museums and archives)
CIS ¹⁴⁰	(copyright societies)
Dublin Core ¹⁴¹	(library originated, resource discovery)
GRid	(recording industry)
IFLA FRBR ¹⁴²	(libraries)
IMS ¹⁴³	(education)
International DOI Foundation ¹⁴⁴	(content industries)
IEEE LOM ¹⁴⁵	(education)
MPEG-7 ¹⁴⁶	(audiovisual)
MPEG-21 ¹⁴⁷	(audiovisual originated)
ONIX ¹⁴⁸	(book industry)
P/META ¹⁴⁹	(audiovisual)
SMPTE ¹⁵⁰	(audiovisual)

These schemes, developing from different starting points, are all converging on the “barriers” we have identified. To some degree, each is finding that is has to become multi-media, multi-function, multi-level, multi-lingual and technology neutral. As convergence renders the traditional sector divisions increasingly meaningless, they will inevitably need to interoperate with one another substantially. In future, essentially the same metadata about, for example, a web document, may need to be handled within each of these schemes, and many more.

¹³⁸ See: Lagoze, Hunter (2001).

¹³⁹ International Committee for Documentation of the International Council of Museums (ICOM-CIDOC) — Web Site:
<http://www.willpowerinfo.myby.co.uk/cidoc/>.

¹⁴⁰ International Confederation of Societies of Authors and Composers (CISAC)
— Web Site: <http://www.cisac.org>.

¹⁴¹ See above Fn. 131

¹⁴² See: IFLA (1998).

¹⁴³ IMS Global Learning Consortium, Inc — Web Site:
<http://www.imsproject.org/>.

¹⁴⁴ International DOI Foundation — Web Site: <http://www.doi.org>.

¹⁴⁵ See: IEEE.

¹⁴⁶ See: MPEG-7 (2001).

¹⁴⁷ See: MPEG-21 RDD (2003).

¹⁴⁸ See: BIC.

¹⁴⁹ See: Hopper (2002).

XIX.2 Creating Interoperability: Mapping Metadata

If two metadata schemes are in use and a DRM application needs access to both, then a mapping between them will need to be created. Mappings are concerned with meanings, not names; entities can have different names in different schemes, and the same word can mean different things in different schemes. Simple one-to-one mappings between schemes are commonplace; some mappings are very precise, and others loose. However, the more schemes come into play, the more one-to-one mappings will be required, each of which is costly in resources and likely to be less than adequate. With the rapid growth of metadata schemes this is becoming an increasing problem. When there are N schemes, there are $\frac{N}{2}(N - 1)$ one-to-one mappings needed; this rapid growth in complexity can be eased by mappings through a central point or dictionary: each scheme then requires mapping once (N schemes require N mappings).

The emergence of the indecs Data Dictionary (iDD), as articulated in the MPEG-21 RDD, offers precisely such an extensible yet firmly grounded ontology for such a dictionary. It should be possible to create any required one-to-one mappings making use of the iDD ContextModel structure. The DOI's Metadata System is built on this basis: all terms used by DOI Application Profiles must be mapped into the iDD, establishing the relationship between a term and all other terms used by APs, and is the way in which semantic integrity is achieved. This is a painstaking process, but it is typically a once-off for each term or scheme, with subsequent maintenance required only when new terms are added, or amendments made. Mechanisms for modifying mappings, adding and deleting new Terms are provided for by the iDD, although of course the consequences of such changes can be serious. A mapped term becomes a part of the Dictionary. The iDD structure is capable of recognizing any number of contextual meanings, and as new ones are identified in the course of mapping, they are placed in their appropriate place in the dictionary and ontology.

The level of granularity described above is unnecessary if only two or three schemes are being mapped. However, the fundamental assumption underlying the iDD and the DOI Metadata System is that in time there will be many applications whose metadata requires integrating at various levels, whether simply at the DOI Kernel level or to support more complex searching and processing. Semantic integrity on such a scale appears unachievable without a central tool such as the iDD, for two simple reasons: precise mapping depends upon at least one of the mapped schemes having a rich underlying model in which to precisely locate the others' terms; and multitudinous one-to-one mapping schemes are unsupportable both economically and in terms of maintaining consistency.

A mapping cannot produce unambiguous or precise mappings if the terms used in the source scheme are themselves ambiguous or imprecise. iDD can accurately describe the ambiguity and leave the resolution to users. What iDD should be able to achieve is accurate mapping as far as the source data allows, producing

¹⁵⁰ Society of Motion Picture and Television Engineers — Web Site:
<http://www.smpte.org/>.

considerably better results than a host of many-to-many mappings based on more limited models and varying techniques. The iDD contains the logic and data to support many kinds of processing, such as data transformations or the creation of scheme-to-scheme maps, but these will require the development of application software and business processes. Contextual mappings provide one of the necessary bases for semantic interoperability, but do not provide everything.

Mapping in this precise way is practically focussed on entities that can be clearly defined and have a role in the resource-based functions typical of current DRM applications. Mapping complex concepts is possible, but concepts like “digital rights management” are not currently consensually precisely defined; there is a majority view that it is digital management of rights, rather than management of digital rights, but beyond that “DRM is something to do with managing, something to do with rights and something to do with the digital environment. But not necessarily” (Godfrey Rust). Focussing on what is practically definable through practical tools like the MPEG-21 RDD, rather than arguing about “what is” DRM as a whole, is likely to produce useful implementations.

XX MPEG-21 and Other Activity

The ISO/IEC/MPEG-21 standard multimedia framework activity¹⁵¹ is one of the most promising practical developments in DRM, which has embraced a structured view of identifiers and metadata, specifically by using the indecs metadata framework as a basis for well-formed structured metadata through the MPEG-21 Rights Data Dictionary. The details of this extensive standards effort are beyond the scope of this chapter, but it is useful to comment on the relationship of MPEG-21 to some of the concepts and efforts which have been discussed.

The MPEG-21 world consists of *Users* who interact with *Digital Items*. A Digital Item can be anything from an elemental piece of content (a single picture, a sound track) to a complete collection of audiovisual works: an MPEG “digital item” can be considered a sub-set of what DOI calls a “Digital Object”. The specification of “identifier” in the MPEG-21 DII¹⁵² is: “Digital Items and their parts within the MPEG-21 Framework are identified by encapsulating Uniform Resource Identifiers (URIs), into the Identification Description Scheme” — that is, it provides another “identifier specification”, adopting URI, rather than a detailed specific implementation. Hence identifier implementations such as DOI which are specified as a URI can be used in MPEG-21 to identify Digital Items.

Whilst the framework for DRM rules for “consumption” specification by end user devices are laid down in MPEG-21 part 4¹⁵³, the full mechanism for expressing identified and described resources in a rights environment (essentially a messaging standard for permissions) requires the MPEG-21 part 5 “Rights Expression Language” (REL) — significantly influenced by and largely based

¹⁵¹ See: MPEG-21 Visions, Technology & Strategy (2001).

¹⁵² See: MPEG-21 DII (2002).

¹⁵³ See: Koenen (1999); MPEG-4 Overview (2002).

on ContentGuard’s Extensible Rights Mark-up Language, XrML¹⁵⁴) — and the underlying MPEG-21 part 6 Rights Data Dictionary (RDD) standard¹⁵⁵, each of which are in development at the time of writing. Two significant points should be noted:

- The “REL” is misleadingly named, from the point of view of the content industries — whilst very useful, its scope is restricted to “rights” which can be practically expressed as some *action* in a digital context, rather than *legal* concepts like “copyright” which have no direct executable equivalent; and hence it is rather more a “network privileges language” — does the user have the “right” to delete, install, execute, etc. (verbs such as copy are derived from the basic framework but are not root verbs.)
- The RDD is built on the basis of the indecs Data Dictionary (iDD) referred to earlier as a useful mapping tool, by a group of organisations representing both commercial interests and trade bodies across the content industries which sponsored a Consortium¹⁵⁶ to develop the indecs framework into a Rights Data Dictionary. Hence articulating the MPEG-21 RDD through a practical operating registration authority (which is necessary, since the dictionary is by definition dynamic) will provide a common basis for mappings for DOI (which already sues the preliminary version) and other identifier system implementations in DRM.

Other DRM consortium standards activities have been launched in specific sectors, one of the most notable being the Open Mobile Alliance¹⁵⁷, whose standardisation work in “OMA Download” include both DRM (building on the Open Digital Rights Language proposal¹⁵⁸ submitted to W3C¹⁵⁹, which was rejected by the MPEG-21 review process) and the over-the-air delivery of generic content. OMA has the support of Nokia, a significant player in the mobile delivery of content.

In the commercial DRM market, a number of proprietary interests and solutions are currently being actively promoted: these include Microsoft (which is aligned with ContentGuard), IBM, Macrovision (a leading player in DRM for consumer media), and Sony and Phillips who have recently jointly acquired Intertrust. There are many other smaller companies developing technologies for securing digital media. Some of these can be seen as implementation layers on top of a standards framework such as MPEG-21; others adopt a non-MPEG approach (such as the use of ODRL by the Mobile Nokia). This has led some commentators to state that DRM standards will be driven by the victor in a commercial shoot-out, rather than it an industry trade association or standards committee¹⁶⁰. Proprietary solutions suffer from the obvious problems of technology lock-in,

¹⁵⁴ XrML Web Site: <http://www.xrml.org/>.

¹⁵⁵ See: MPEG-21 RDD (2003); Paskin (2001).

¹⁵⁶ See: DOI News (2001).

¹⁵⁷ Open Mobile Alliance Web Site: <http://www.openmobilealliance.org/>.

¹⁵⁸ The Open Digital Rights Language Initiative Web Site: <http://odrl.net/>.

¹⁵⁹ See: W3C (2002).

¹⁶⁰ See: Bulletin (2002).

obsolescence, and interoperability — despite which, it is certainly possible that one of these might become a de facto standard.

Whatever the solution or solutions which are chosen, it remains essential to have a logical and consistent application of identifiers and metadata in an underlying extensible framework (such as indecs) which can be used to map whatever solution seems to be the more popular to those solutions which are less popular.

XXI Acknowledgements

Parts of this article are based on material from The DOI Handbook, including earlier contributions by Mark Bide (Rightscom Ltd.), Godfrey Rust (Data Definitions) and Laurence Lannom (Corporation for National Research Initiatives).

2.3.2 Authentication, Identification Techniques, and Secure Containers — Baseline Technologies

*Gabriele Spenger*¹⁶¹

Abstract: The commercial distribution of multimedia content over the Internet demands high security mechanisms. There is not only the possibility of third persons intercepting the communication, but also the risk of malevolent hackers faking the identity of registered users. This paper describes mechanisms that prevent such attacks. First an overview of cryptographic algorithms is given. After that the terms identification and authentication are defined and examples of techniques and protocols for user and content authentication are given. The next sections give a short overview of connection based security protocols and the secure container technology used in DRM systems. The final section shows some security aspects of client DRM systems.

I Introduction

The quickly growing E-commerce market is one of the most demanding applications for security technologies. The transfer of electronic versions of goods like

- Audio (music albums, songs, audio books)
- Video (movies, video clips)
- Text (newspapers, magazines, literature)
- Computer software (games, applications)

over an open network like the Internet often use “secure containers” based on secure cryptographic mechanisms, because not only virtual goods but also real money is involved. But not only the transfer of the goods over the Internet is important, it is also the protection of the usage rights and copyrights that are of particular interest. The variety of business models is large: there are pay-per-view models, subscriptions, time-restricted usage or free availability of quality reduced try-versions of the material. For all business and communication models there are features that have to be provided by the underlying multimedia platform. One of them is the possibility to ensure that content that has been paid for is only available to the correct user that has paid for it.

For these and other applications security mechanisms have been developed to make communication possible between parties that can be sure of the identity of each other. But the protection of the copyrights does not end with the successful transmission of content-related information, there also has to be control over the use of the content itself. Most critically, this has to be as long as the material is in the hand of the user and commercially valuable.

The security of transmission, the authentication of users and the protection of usage- and copyrights are all based on the same cryptographic operations and algorithms.

¹⁶¹ University of Erlangen-Nürnberg.

II Overview of Cryptographic Algorithms

A cryptographic algorithm is a mathematic function used for en- and decryption. If the security of such an algorithm is based on the secrecy of its operation, it is called a *restricted algorithm*. Restricted algorithms are mainly of historical interest, as they are not used in current standards anymore and because they are not suited for larger groups of users (or for user groups with a high fluctuation) because they would have to be modified each time a user leaves the group. An even greater problem is that restricted algorithms do not allow independent quality control and standardization because when the algorithm gets into the wrong hands — and the process of standardization makes this very likely —, it will be completely useless.

In modern cryptography these problems are solved by using “keys”. A key is a secret information that is used by the cryptographic algorithm for en- and decryption. This separation of algorithm and key makes it possible that different parties can use the same algorithm and still ensure privacy by using different secret keys. These keys are chosen from a large number of values. The range of possible values is called *key space*. The security of modern algorithms is not based on the secrecy of the algorithm but only on the secrecy of the key and size of the key space. This principle has been introduced by A. Kerckhoffs in the 19th century. The Kerckhoffs principle allows the algorithm to be published and crypto-analyzed independently.

There are two general types of key based algorithms: *Symmetric* and *asymmetric* algorithms. Symmetric algorithms use the same key for encryption and for decryption. Hence, sender and receiver have to agree on a secret key that must not be revealed to outsiders in order to enable a secure communication amongst them. Asymmetric algorithms, also known as public key algorithms, use two different keys. One of these keys is called the “private key” and must be held secret, while the other key is called the “public key” and may be published. The secret key cannot be derived from the public key.¹⁶² As both of these types of algorithms have certain disadvantages (see the following two sections) there are also systems, which combine both types.

II.1 Symmetric Cryptographic Algorithms

In the early seventies the upcoming of increasingly faster computers opened completely new horizons in cryptographic research. Although it was commonly known that the military was communicating with special cryptographic devices, only a few were familiar with the science of cryptography. Several small companies produced and sold cryptographic devices that worked differently and were not compatible. There was virtually no public information about the security of these devices, because no independent institution existed that would have been able to test (i.e. try to break) the algorithms used.

¹⁶² See: Schneier (1996).

In 1972 the National Bureau of Standards (NBS, now: National Institute of Standards and Technology, NIST) in the USA started a program for the secure storage and transmission of data. A part of the program should be the standardization of a cryptographic algorithm. This algorithm would have to be able to be publicly tested and devices based on it should be able to work together. And because the algorithm would be publicly available during the standardization process, implementing it into devices would be comparatively easy — also for non-cryptologists.

The NBS published a call for proposals in 1973 listing several requirements. Some of these were:

- High security,
- Complete specification,
- Exportability,
- Efficient usability,
- The possibility of inexpensive implementation as electronic circuit and
- The security of the algorithm should not depend on the nondisclosure of the algorithm, but on the secrecy of the key.

The interest in the call for proposals was high, but none of the candidates that responded to the call fulfilled all criteria. As a result the NBS published a second call (1974) and this time a promising proposition was turned in that was based on a cryptographic algorithm from IBM: “Lucifer”. Lucifer was complicated and consisted of many steps, but the single steps were straightforward. It worked only with logical operations on small bit groups, which meant that it could be implemented quite efficiently in hardware. The NBS asked the National Security Agency (NSA) for support to examine the security of the algorithm and to verify if it would be suitable as a national encryption standard. The NSA categorized the algorithm as acceptable after some changes were made: the key length was reduced from 128 bit to 56 bit and the so-called S-boxes (see the following subsection) that were used in the algorithm were changed.

The algorithm was called *Data Encryption Standard* (DES) and was released as a National Standard in the US in 1976.

Data Encryption Standard (DES)

The DES is a block cipher using a 56 bit key to encrypt 64 bit blocks of plain text into 64 bit blocks of cipher text (or decrypt 64 bit blocks of cipher text into 64 bit blocks of plain text when operated as a decrypt engine). It uses 16 key dependent “rounds” of several simple calculations. Additionally, before the first and after the last round a bit-by-bit transposition (permutation) is performed; the final permutation reversing the first one. As DES is a “Feistel network”¹⁶³ the 64 bit blocks are divided into equal sized left and right parts and each round has the following sequence:

$$L_i = R_{i-1} \quad \text{and} \quad R_i = L_{i-1} \oplus f_S(R_{i-1}, K_i)$$

Figure 1 shows the structure of DES.

¹⁶³ See: Feistel (1973); Feistel (1974).

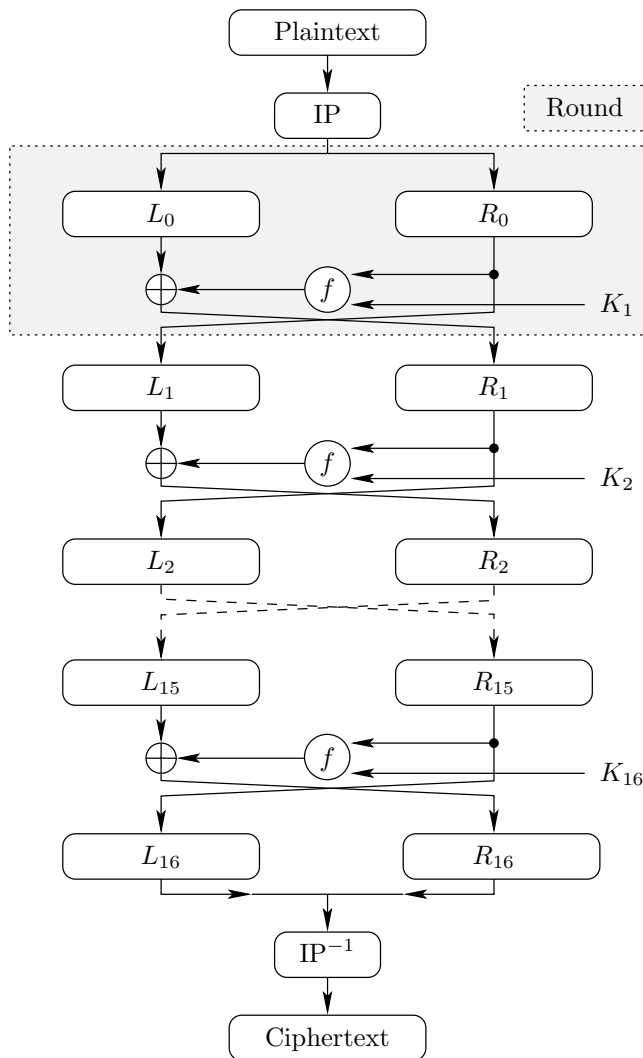


Fig. 1. The Structure of DES.

Where f is a function that changes its operation depending on the key and the round as follows:

- Select 48 bit from the 56 bit key.
- Extend the right part R_i of the input block from 32 to 48 bits.
- Calculate the exclusive or (XOR) of these two 48 bit sequences.
- The result of the XOR is then transformed into a 32 bit sequence using eight so-called Substitution (or S) boxes.
- The resulting 32 bit sequence is then permuted. This transformation is defined by so-called P-boxes (Permutation boxes) that are simply a certain order of the numbers from 1 to 32.

- The final 32 bit sequence is XOR'ed with the left input block part L_i and results in the right input part R_{i+1} of the next round.

In the following is more detailed enumerate of the single steps:

Initial and Final Permutation:

The permutations in the beginning and at the end of the algorithm have no cryptographic relevance. Presumably they have been introduced to facilitate the implementation in hardware. In the mid-seventies it was not easily possible to calculate using 64 bit sequences.¹⁶⁴

Key Transformation:

At the beginning of each round the 56 bit key is divided into two 28 bit sequences. Each sequence is rotated (i.e. shifted) for one or two bits depending on the round number. After that the two 28 bit sequences are assembled to a 56 bit key again. Then 48 bits of the 56 bits are selected according to a fixed scheme and permuted simultaneously. As this step reduces the number of bits it is called “compression permutation”. Because of the key transformation every round of the algorithm uses a different key.

Half Block Extension:

The 32 bits of the right half of the input block are spread to 48 bits by a fixed transformation. As this step increases the number of bits it is called “expansion permutation”.

The cryptographic background of the expansion permutation is the so-called “avalanche effect”: every changed input or key bit influences the cipher text after as few rounds as possible. This is also the reason why it is better to compress the key and expand the input each to 48 bits than XOR'ing the input block half with a key compressed to 32 bits.

The expansion permutation is displayed in figure 2:

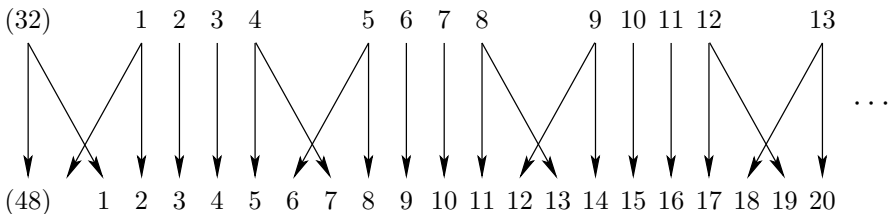


Fig. 2. The Expansion Permutation of DES.

S-Boxes

The 48 bit block resulting from the last step is divided into 8 groups of 6 bits each. These groups are transformed each with a different S-box. The eight S-boxes are the most critical part of DES. Each S-box consists of a table with 4

¹⁶⁴ See: Schneier (1996).

rows and 16 columns and transforms 6 input bits into 4 output bits. An example for a DES S-box is shown in Figure 3.

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

Fig. 3. S-Box Number 5 of DES.¹⁶⁵

The S-box is applied in the following way: If the input consists of the six bits b_1, \dots, b_6 , the number formed by b_1 and b_6 (2 bits = 4 possible values) determines the row of the table and bits b_2, \dots, b_5 determine the column. The number in the resulting row and column is the output value. Figure 4 shows a block diagram of a DES round.

The DES algorithm appears quite complicated, but there are good reasons for the design. The algorithm can be realized in hardware very efficiently, because there are no additions and above all no multiplications. The algorithm consists only of bit shifts, fixed permutations and XOR operations. The several steps each have their specific purpose:

- The expansion permutation and the P-box lead to the avalanche effect.
- The P-boxes also have the purpose that each input bit is transformed by a different S-box in each of the rounds.
- The S-boxes lead to non-linearity and immunity against differential crypt analysis.
- Rotation and compression permutation have the purpose that a change of a key bit influences all input bits already after a few rounds.¹⁶⁶

There are three known kinds of attacks known against the DES algorithm:

- Brute force,
- Differential crypto-analysis and
- Linear crypt analysis.

Today, the only practicable attack is the brute force attack. Brute force means, however, trying out *all* 2^{56} possible keys by decrypting the cipher text and testing the resulting plain text for its meaning. In 1996 the RSA Data Security, Inc. set up a challenge for the successful retrieval of a DES key. This was achieved after six months using the idle processor times of computers connected by the Internet. After this first initiative a second challenge was started in February 1998, which was won after only 39 days. 22,000 users with 50,000 computers were involved and had already tried out 85% of the possible keys before the correct key was found. This gave already an indication that DES was not secure enough anymore. The last doubt was eliminated after the Electronic Frontier

¹⁶⁵ Instead of the numbers from 0 to 63 the number of the respective entry in the table is used.

¹⁶⁶ See: Schneier (1996).

Foundation (EFF) built a machine that was able to break a DES key in an average of only $4\frac{1}{2}$ days. The machine was developed by a team of ten people in only 18 months and the budget of the whole project was just US\$ 250,000.¹⁶⁷

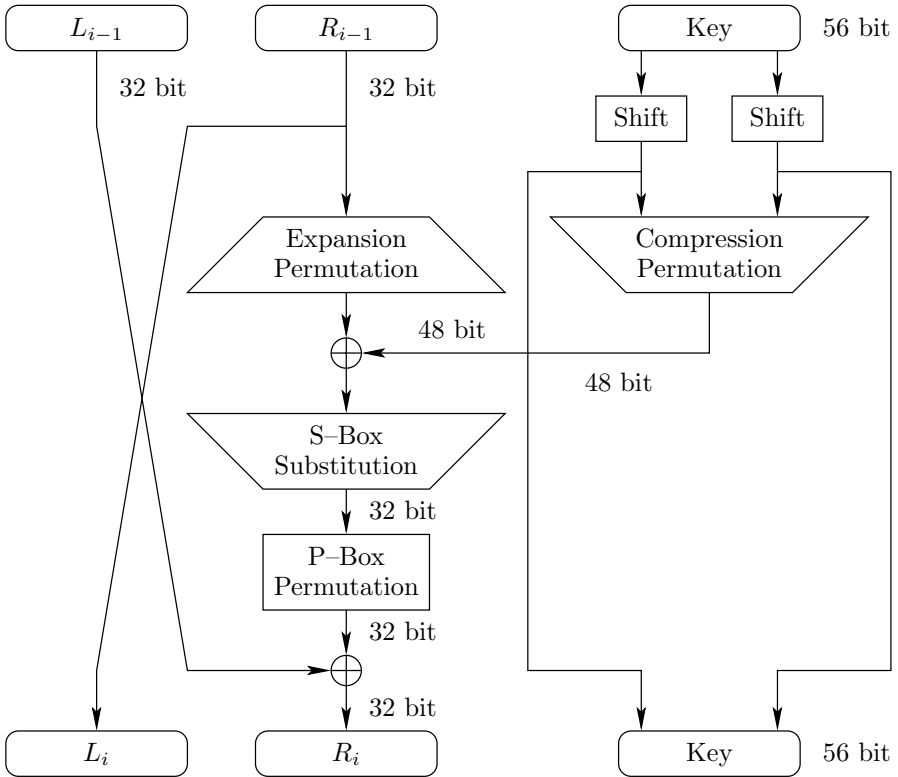


Fig. 4. One Round of DES.

In 1997 — even before the DES was “broken” for the first time — the NIST started the search for a successor of DES that was to be called Advanced Encryption Standard (AES). The requirements for this standard were:

- Symmetric block cipher with a block length of at least 128 bits with key lengths of 128, 192 and 256 bit.
- Suitable for hard- and software implementation.
- Low demand for processing power and memory resources (suitable for e.g. smart cards).
- Resistance against all known cryptographic attacks.
- No patents and no license fees, usable by everybody.

Most leading cryptologist in the world participated in the call for proposals. 15 algorithms were presented on the first conference 1998 and extensively examined and analyzed on the second conference in March 1999. In October 2000 the

¹⁶⁷ See: Wobst (2001).

NIST made a decision and chose the Rijndael algorithm, named after its Belgian developers Vincent Rijmen and Joan Daemen.

Rijndael (AES)

The Rijndael algorithm is based only on byte substitution, byte permutation and the XOR operation, which makes the algorithm extremely easy to implement in hardware. In the following the algorithm is described for 128 bit input blocks and 128 bit key length.

The input block consists of 16 bytes, which are written into a 4×4 matrix called states. At the beginning of the first round of the algorithm the plain text bytes are in such a state. Every round changes the content of the state. After the 10th and final round the matrix contains the cipher text. Furthermore, 10 round keys are generated from the 128 bit key and also written into 4×4 matrices. If Rijndael is used with 192 or 256 bit key length, 4×6 respective 4×8 state matrices are used. Also the number of rounds is changed from 10 to 12 or 14, respectively.

II.2 Asymmetric Cryptographic Algorithms

The concept of asymmetric encryption (also known as public key cryptography) was independently invented by two teams: Whitfield Diffie and Martin Hellman on the one side and Ralph Merkle on the other.

The most significant idea is that the keys are used in *pairs* as encryption and decryption key. The two keys are called *public key* and *private key* and it is not possible to derive the private key from the public key while the public key is derived from the private key.

Hence, this family of algorithms is called asymmetric and allows the following procedure:

A user Bob generates a pair of keys consisting of the public key and the private key. Then he publishes the public key to all the other users of the network. If he encrypts a message with his private key, everybody else can decrypt the message and can be sure that the message is sent by him. The other users can encrypt a message with Bob's public key and can be sure that only Bob is able to read it, because only he knows the required private key.

This idea was first presented on the National Computer Conference in 1976 by Diffie and Hellman¹⁶⁸. Many cryptographic public key algorithms have been published since 1976, but only a few have proven to be as practicable and secure as the Diffie–Hellman algorithm. Only three newer algorithms were versatile enough to be serious contenders in the area of asymmetric cryptography: RSA, El–Gamal and Rabin. RSA has become, in fact, the most widely used asymmetric algorithm. It is named after its inventors Ron Rivest, Adi Shamir and Leonard Adleman.¹⁶⁹

¹⁶⁸ See: Diffie, Hellman (1976).

RSA

The security of RSA is based on the difficulty of the factorization of great numbers. Public and private key depend on a pair of great prime numbers (with a length of 100 to 200 digits). Table 1 shows the schemes used to generate the keys and to encrypt and decrypt a message.

Public Key	n is the product of two primes p and q (p and q must be kept secret) e is relatively prime to $(p-1)(q-1)$
Private Key	$d = e^{-1} \pmod{(p-1)(q-1)}$
Encryption	$c = m^e \pmod n$ (m is the message)
Decryption	$m = c^d \pmod n$

Tab. 1. RSA Encryption.

II.3 Hybrid Systems

Because asymmetric ciphers are significantly slower than symmetric algorithms¹⁷⁰, they are not suited for encrypting and decrypting large amounts of data in short times. For such tasks, symmetric algorithms such as DES and AES are much better suited. Hence security systems often use symmetric algorithms to encrypt and decrypt the message, while asymmetric ciphers are used to encrypt the transmitted key. This allows the two parties to exchange the so-called session key (i.e. the key to encrypt/decrypt the message) during their communication.

III Identification and Authentication

To establish a secure communication it is important to determine who the communication partner is. This identity is usually expressed through a unique identifier comprising various attributes such as the name, age and national insurance number of a person. Often, the unique identifier is represented through a serial number or string.

But identification only recognizes who somebody *claims* to be. For *secure* communication this is not enough. If we communicate with a malevolent hacker we can expect him to send fake identification information. It is therefore important to *verify* the information the communication partner transmits, so that no other person can pretend to have the same identity.

¹⁶⁹ See: Schneier (1996).

¹⁷⁰ Hardware implementations of RSA are about 1,000 times slower than DES and Software implementations are still about 100 times slower than DES. Although these numbers may change in the future, it can be expected that RSA will never reach the performance of symmetric algorithms. See: Schneier (1996).

In every-day life situations it is generally no problem to verify, if a communication partner is indeed the person we want to communicate with and if the information he gives us reaches us unmodified. We achieve this e.g. by recognizing the communication partner's face and/or voice. For electronic communication, however, the situation is different. There are no inherent means to associate received bits to a certain sender. Data bits do not have unique properties like voice timbre or face shape. As the ability to associate content non-ambiguously with a certain sender is a fundamental requirement for secure communication — and therefore for DRM systems —, mechanisms are needed to provide this functionality. These mechanisms are covered by the term *authentication*.

There are two important applications of authentication:

- User authentication and
- Message authentication.

The former ensures that the communication partner is indeed the one we want to communicate with. The latter secures the integrity of the transmitted message.

Taken to a DRM context the following scenario could be imagined: A user contacts a multimedia server and requests a music file for downloading. The server ensures by user authentication that the request is from the registered user Alice who has permission to download the file. The server then gets a request from Alice to purchase several other music files and sends her the price and the bank account she has to transfer the money to. By *message authentication* Alice ensures that the account number has not been corrupted by a malicious hacker who wants Alice to transfer the money to him instead.

The two applications of authentication usually go hand in hand. It is not very useful if the origin of a message has been verified, but the contents of the message has been corrupted by somebody else during transmission. On the other hand it also makes little sense to verify that the received message is identical to the one the sender has sent if there is no proof that the sender is really the person we expect the message to come from. User and message authentication are based on the same cryptographic algorithms.

User Authentication Techniques

One easy method to verify the identity of a communication partner is to agree on a common secret. If only two communicating parties share the secret they can make sure that they communicate with each other by verifying that the respective communication partner — and only him — knows the secret. This method can be realized by symmetric cryptography.

The problem with this method of authentication is that the secret key must have been exchanged before the communication takes place. To do this in a secure way is normally not an easy task. If the secret key falls into the wrong hands, somebody else could fake the identity of the desired communication partner by “proving” that he knows the secret key. As every communication over a network may be intercepted by somebody else the secret key is often exchanged via an alternative medium (fax, telephone, mail). This usually takes time or careful

planning and the security of the alternative medium may be questionable. Any effort to establish a secure connection over a network is vain, if the secret key is written on a piece of paper on the office desk that can be read by everybody.

Another problem is that separate secret keys are needed for every pair of parties that want to authenticate each other in a communication. This leads to an additional overhead either to create and exchange secret keys for every communication or to administer the existing keys for each pair of communication partners.

Public key cryptography makes user authentication much easier. In public key cryptographic systems each user has, as described above, a pair of keys. One key is public and is accessible by all users, for example, from a database. The other key is private and only known to the respective user. Any data encrypted with the private key can only be decrypted with the public key and any data encrypted with the public key can only be decrypted with the private key. It is not possible to decrypt the data with the key it was encrypted with and it is not possible to reconstruct the private key from the public key. This way it is ensured that data intended for a user (and encrypted with the public key) can only be read by him, while data which can be decrypted with the user's public key is ensured to be sent by him (see section on Secure Containers below).

With public key cryptography the authentication of a communication partner is possible without the exchange of any additional information: If Alice wants to be sure to communicate with Bob, she encrypts the message she wants to send to Bob with his public key. Eve, who overhears the communication, does not know Bob's private key and is not able to decrypt the message. An enumerate of the protocols used for user authentication as they are defined in the X.509 framework below.

But public key cryptography for authentication also has its drawbacks. Firstly the complexity of the used algorithms is much higher. This may lead to problems on hardware platforms with low CPU power (e.g. portable devices, smart cards etc.). And, secondly, then there is also a certain additional overhead for administration, because there has to be a trustworthy instance that administers the public keys for the users.

Message Authentication Techniques

There are several methods for message authentication. A simple one is based on symmetric key encryption. In order to ensure the integrity and authenticity of a non-encrypted transmitted message, the receiver needs additional information from the sender for verification. This additional information is called cryptographic checksum or Message Authentication Code (MAC)¹⁷¹. The protocol to generate the MAC is based on secret keys known on sender and receiver side and a cryptographic algorithm. The theory is similar to the theory of hash functions.

A hash function is a mathematically defined function that generates a fixed length output value (hash value) from a variable length input text. The hash

¹⁷¹ See: Beutelspacher (1996).

sum is usually significantly shorter than the input text. A very simple hash function is, for example, a function that returns a one byte value calculated as the XOR-function on all input bytes. This hash function is, however, not suitable for authentication purposes, as it is very easy to generate an input text to match a given hash sum.

Several algorithms have been standardized that provide the necessary security, most commonly used are the Message Digest number 5 (MD5) by Ron Rivest and the Secure Hash Algorithm (SHA) by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). The main design goals for these algorithms are the same:

- Practical impossibility to create two messages with the same hash,
- Brute force being the most efficient attack,
- Simplicity,
- Low memory and processing power requirements.

Both algorithms also follow the same principle: The input is segmented in blocks with a length of 512 bit. Then four rounds of several operations are performed on these blocks (with 16 operations for MD5 and 20 for SHA). The operations cover logical operations, bit shifting and arithmetic operations. The results of the calculations on each block are combined to get the final hash value (128 bit for MD5 and 160 bit for SHA)¹⁷².

Another way to verify the authenticity of a message uses asymmetric key encryption. Digital signatures work with asymmetric key encryption, but they leave the data unencrypted. Instead they use the encryption algorithm to calculate a hash. This hash is appended to the message and can be used to verify the authenticity of the content.

III.1 The ISO Authentication Framework

In 1988 the International Organization for Standardization (ISO) began working on an authentication framework with the goal to define a common standard for authentication. The result was adopted in 1993. The scope of the authentication framework is to provide a protocol for authenticating individuals over an open network. In this framework, also known as X.509 protocol, public key cryptography was recommended. In the specification no specific algorithm for security and authentication is prescribed, but RSA is “recommended”¹⁷². Instead, the ISO Authentication Framework provides interfaces for many security algorithms and hash functions.

Public Key Certificates

The most important part of the X.509 protocol consists of its structure for public key certificates. A trustworthy certification authority (CA) assigns an unique name to every user and publishes a signed certificate with the user name and the user’s public key. The signature appended to this certificate is generated from the CA’s secret authentication key and the parameters held within the CA’s own

¹⁷² See: Schneier (1996).

authentication certificate. A CA may generate and sign its own authentication certificate, or the CA may be provided with its certificate by a higher level CA, leading to a hierarchy of CAs with a master CA at the top and the user at the bottom. Figure 5 shows a X.509 certificate.

Version	Serial Number	Algorithm Identifier	Issuer	Period of Validity	Subject	Subjects's Public Key	Signature
		Algorithm Parameters		Not Before Date Not After Date		Algorithm Parameters Public Key	

Fig. 5. An X.509 Authentication Certificate.

The “version” field describes the format of the certificate. The “serial number” is an unique number for the certificate within the CA that issued the certificate. The next field “algorithm identifier” denotes the algorithm that was used for the signature of the certificate and some further necessary information. “Issuer” contains the name of the CA. The field “period of validity” consists of two dates between which the certificate is valid. “Subject” denotes the name of the user. Under “subject’s public key” the name of the algorithm, the necessary parameters and the public key are listed. The final field “signature” contains the signature of the CA.

III.2 Usage Scenario: Authentication in a CA–Hierarchy

If Alice wants to communicate with Bob she first looks up Bob’s certificate in a database. Then she verifies the authenticity of this certificate. If Bob and Alice have their certificates from the same CA this is easy. Alice simply has to verify the CA’s signature on Bob’s certificate.

If Bob and Alice have their certificates from different CAs, the situation is more complicated. In a tree–like structure, every CA has a certificate from a higher level CA up to the master CA. Alice has to verify all the certificates from Bob’s certificate up to a common CA from which there is a certification path down to her own CA. From this common point she has to verify the certificates going down to her own CA. Figure 6 shows an example for such a scenario.

If Alice wants to send a message to Bob, Bob first sends his certificate to Alice. This certificate is signed by Carol. Alice can verify this signature with Carol’s public key. This key is signed by Dave. Dave’s key is not only signed by Eve, but also by Frank. Frank’ key is signed by George and George’s key is signed by Alice herself. This is how Alice can verify that Bob’s certificate is valid.

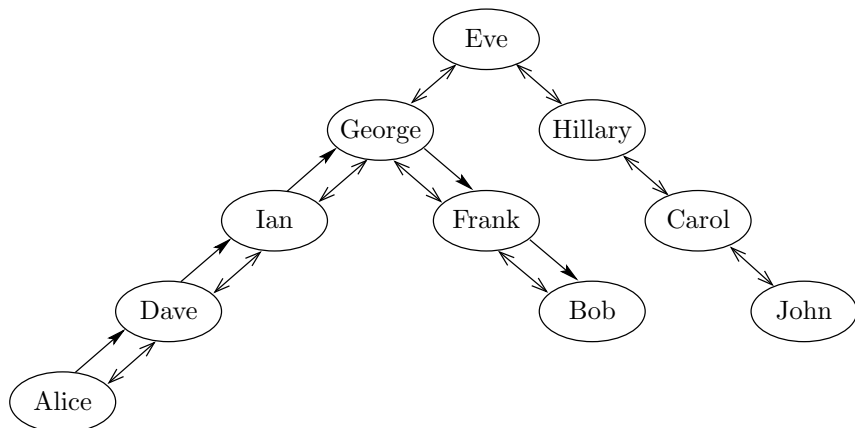


Fig. 6. Sample Certification Hierarchy.

Authentication Protocols

The X.509 standard¹⁷³ defines several authentication protocols that describe the steps necessary for a secure user authentication. If Alice wants to communicate with Bob, she first accesses a database and gets a “certification path” from Alice to Bob and Bob’s public key. Alice now has the choice between three authentication protocols:

The *one way protocol* consists of a single communication step from Alice to Bob. Bob’s and Alice’s identity is confirmed and the integrity of the transmitted information is ensured. The protocol furthermore prevents replay attacks (faking an identity by sending copies of messages of a former communication). It has the following steps:

- (1) Alice generates a random number R_A
- (2) Alice generates a message $M = (T_A, R_A, I_B, d)$, where T_A is Alice’s time stamp, I_B Bob’s identity and d an arbitrary information. The message may be encrypted with Bob’s public key for security reasons.
- (3) Alice sends $(C_A, D_A(M))$ to Bob. (C_A is Alice’s certificate; D_A is the common point in the certificate tree.)
- (4) Bob verifies C_A and gets E_A . He ensures that the key has not expired. (E_A is Alice’s public key.)
- (5) Bob decrypts $D_A(M)$ with E_A . By that he has verified both Alice’s signature and the integrity of the signed information.
- (6) Bob verifies that the I_B in M is correct.
- (7) Bob examines T_A in M and checks if the message is up to date.
- (8) To enhance the security even more Bob can look up R_A in a database of old random numbers to be sure that the message is not a copy of an old message (replay attack).

The *two way protocol* consists of a one way protocol followed by a very similar

¹⁷³ See: X.509 (1989).

one way protocol in the other direction from Bob to Alice. Steps (1) to (8) of the one way protocol are followed by the following steps:

- (9) Bob generates a random number R_B
- (10) Bob generates a message $M' = (T_B, R_B, I_A, R_A, d)$, where T_B is Bob's time stamp, I_A is Alice's identity and d is an arbitrary information. R_A is the random number Alice has generated in step (1). The message may be encrypted with Alice's public key for security reasons.
- (11) Bob sends $D_B(M')$ to Alice.
- (12) Alice decrypts $D_B(M')$ with E_B . By that she has verified both Bob's signature and the integrity of the signed information.
- (13) Alice verifies that the I_A in M' is correct.
- (14) Alice examines T_B in M' and checks if the message is up to date.
- (15) To enhance the security even more Alice can look up R_B in M' in a database of old random numbers to be sure that the message is not a copy of an old message.

The *three way protocol* achieves the same as the two way protocol but manages it without the time stamp. Steps (1) to (15) are identical to the two way protocol but with $T_A = T_B = 0$. The following steps are appended:

- (16) Alice compares the received random number R_A with the R_A she has sent Bob in step (3).
- (17) Alice sends $D_A(R_B)$ to Bob.
- (18) Bob decrypts $D_A(R_B)$ with E_A . By that he has verified Alice's signature and the integrity of the signed message.
- (19) Bob compares the received random number R_B with the R_B he sent Alice in step (10).

IV Securing Connections

The growing e-commerce market in the past years would not have been possible without the Internet. The Internet is ideal for the commercial transmission of information and electronic goods, because it is available for nearly everybody, it is fast and, apart from ISP charges and hardware costs, it is virtually cost free. The security operations explained in the past sections are especially important for such an open and unprotected network like the Internet. In order to remedy security issues, protocols have been developed to perform authentication and secure transmission for the Internet. In the following, a short overview of an example of such a protocol is given.

IV.1 Secure Socket Layer (SSL)

The Secure Socket Layer (SSL) has been developed in 1994 by Netscape together with its first Internet browser. The goal was to provide a flexible and easy to use protocol for securing client-server connections. Today SSL is the most commonly used security protocol for the Internet. SSL was, however, an early step in the

area of Internet security and therefore it had several weaknesses that have been removed in the current version 3.0. The best known weakness of an earlier version, SSL 2.0, was not in the standard itself but in the reference implementation SSLRef by Netscape, that was published in 1995. It contained an error in the random number generator that undermined the security. Nevertheless, the 2.0 protocol also contained a series of weaknesses, that have since been addressed and have been removed in SSL version 3.0. These weaknesses are:

- Security weaknesses — SSL 2.0 is prone to certain “man-in-the-middle” attacks. The attacker sits in the middle between client and server and modifies a message from the server to the client in a way, that only 40 bit encryption of subsequent messages is established. Encryption with a 40 bit key is nowadays not secure enough anymore. A second weakness is the way in which the MAC is calculated. Fortunately, there are no known attacks utilizing this weakness, because the MAC is encrypted afterwards, but nevertheless the MAC calculation has been changed in version 3.0. The greatest weakness, however, was the message authentication in the “export version”. US export regulations demanded the length of the encryption key to be not more than 40 bits long. Hence, the length of the MAC key was shortened to 40 bits as well, which introduced a serious weakness.
- Functional weaknesses — In SSL 2.0 the client can only perform a handshake at the beginning of the connection. A change of the algorithms or the keys *during* the connection was not possible. A second issues for SSL 2.0 was the restriction to flat public key infrastructures. All server certificates had to be signed with the root certificate, because only one certificate could be transmitted in the certification message. Also, the only algorithm used for key exchange and for signing the certificates was the (patented) RSA algorithm. In version 3.0 key exchange algorithms like Diffie–Hellman and Fortezza as well as non RSA–based certificates have been added. In SSL 2.0 no compression schemes were considered. In version 3.0 it is generally possible to use compression, although no compression scheme has been specified up to now.
- Conceptual weaknesses — In SSL 2.0 the data transmission was closely related to the message layer: Every packet contained exactly one handshake message. In 3.0 this unnecessary relation has been removed. SSL records may now contain a part of a message, a whole message or several messages.¹⁷⁴

SSL 3.0 is commonly regarded as an example of a good and stable security standard. The weaknesses of SSL 2.0 have been removed and there are plenty of commercial and free implementations.

Components of SSL 3.0

The fundamental idea behind SSL is to insert an additional security layer above the TCP protocol in the communication model. The task of this record layer is to encrypt and authenticate all data using the given cryptographic parameters before it is handed over to the TCP transport protocol. This way only encrypted data is transmitted over the Internet that is handed over to the record layer on

¹⁷⁴ See: Schwenk (2002).

the receiver side for decryption. An essential strength of SSL is the handshake protocol used for negotiating the cryptographic parameters.

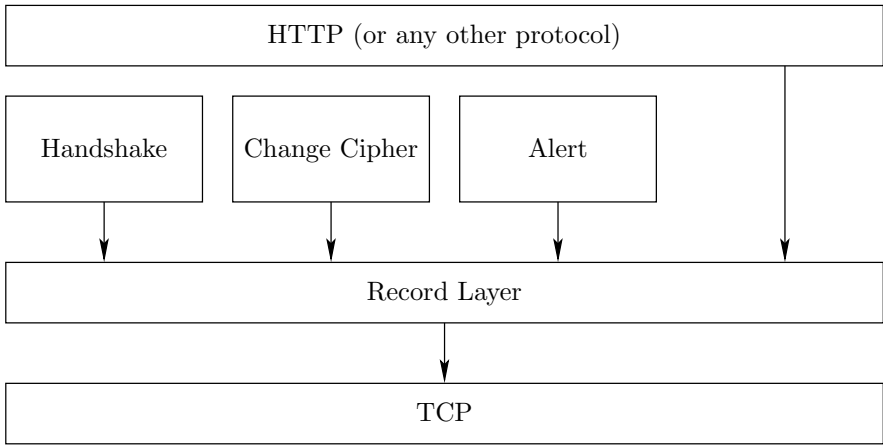


Fig. 7. The Components of the SSL Protocol.

The SSL handshaking is the heart of the SSL protocol and the most complex part of it. It performs the key exchange between server and client, that makes an encrypted communication possible. The base of the handshake protocol is a two way key exchange based on a public key encryption scheme:

- The server transmits its public key to the client (packed into a SSL certificate that also contains the domain name).
- Then the client encrypts a secret random number with the public key of the server and transmits this value to the server. This secret random number is used by client and server for the calculation of the symmetric keys.

V Secure Container

Three important elements of a typical DRM system are file encryption, key management and access conditions. The multimedia content is encrypted using symmetric or hybrid encryption schemes before it is loaded onto the web or streaming server. An enumerate containing (a) metadata describing the content and (b) the conditions and prescriptions for decryption is added to the content file¹⁷⁵. The enumerates are then securely associated with the rest of the file by a digital signature or a MAC. The keys needed for decryption can be downloaded from a special license server. DRM has a great advantage against classical transport encryptions like SSL: The encryption of the content is separated from the

¹⁷⁵ It should be noted that in many DRM systems actually do not package the conditions into the same package as the content itself. Such a separation offers many additional business models that are not possible when the rules and content and packaged together. One example is that it would prohibit to update and change the rules after the secure container has been distributed without re-distributing the content as well.

key management. The encryption can take place on one server, while the key distribution is handled by a different server. The content can be distributed over the whole Internet.¹⁷⁶

DRM protected content reaches the customer in the following way: The content provider prepares the content for the Internet (e.g. as mp3 file, PDF document or an MPEG-4 video). A cryptographic key is generated in a secure environment and the content is encrypted with it. This key is transmitted securely to the license server together with a unique identification of the content. The URL of this and possibly several other license servers is added to the content unencrypted. The content that has been modified in this way is distributed to an arbitrary number of caches and servers in the Internet. The customer can either download the encrypted content and store it, or he can stream the content. The renderer of the content notices, that the content is protected and reads the access conditions and the URL of the license server. Typical access conditions could be “one view for \$2” or “one month of unlimited access for \$10”. The customer can then choose his preferred access offers and his client software connects to the license server. The customer has to identify himself to the license server and gets in exchange the content key.¹⁷⁷

The encryption of the content and the addition of the access conditions and license server URLs can be imagined as putting the content into a locked container. This container is then transported to its destination (the renderer on the client side), where it is unpacked again according to the rules stored in the container. This is the reason why this approach is called *secure container technology*.

VI Security Aspects of Client DRM Systems

One of the weak points of client DRM systems is that the client usually resides in a hostile environment. The user has complete control over the client platform and can try any attack on the client he can think of to try to circumvent the security mechanisms. DRM systems must not only be protected against the corruption of the so-called persistent state variables (e.g. a device ID), but there are also parts of the persistent state that must be protected against unauthorized reading (e.g. encryption keys).

The protection against corruption of the persistent state is often realized by tamper-detection. A tamper-resistant system tries to detect whether attempts are made to use it improperly and stops execution then. This means that state variables read by the system are compared against the values that have been written before. This can only be done by an additional log of write actions. As this log is also a part of the persistent state, the tamper-resistance of a DRM system can usually not be guaranteed.

The protection against unauthorized reading can be provided by encryption of the data with a secret key stored in read only memory. Tamper-detection can, for

¹⁷⁶ See: Kohl (1998).

¹⁷⁷ See: Schwenk (2002).

example, be performed by attaching a Message Authentication Code to each data record. Such a mechanism does not protect against the replay attack, however: A user could backup the persistent data, perform some operations and replace the new persistent data with the one he has as backup. This would make the DRM system “forget” that the operations took place. The user does not even have to understand the structure of the persistent data, as it is replaced as a whole.¹⁷⁸

¹⁷⁸ See: Shapiro, Vingralek (2001).

2.3.3 Digital Watermarking

*Fabien A.P. Petitcolas*¹⁷⁹

There is one aspect of copy control that digital rights management technologies based on encryption do not address. It is the case when the high value content leaves the “digital world”, namely when it is converted to waveforms that can be heard or seen by people. To solve this problem, there has been a growing “interest” on digital watermarking, mainly created by pressure from the content industry on the consumer electronics and the high technologies industries to find ways to better protect copyrights. *Watermarks* are imperceptible marks hidden in multimedia object, including audio visual signals. In a typical content screening system, the client’s media player searches the content for such hidden information. If the secret mark is found, the player then verifies whether a valid license is present. By default, unmarked content is considered as unprotected and is played without any barriers. To be effective, the watermarking technology should be such that breaking a single player or a subset of players does *not* compromise the security of the entire system¹⁸⁰.

In this chapter we will introduce a widely used technique for watermarking audio–visual signals. We will also explain how this technique is being improved to match the requirements imposed for practical use and will show that the state–of–the–art is still far from accomplishing what content owners may expect.

I Basic Blocks for Digital Watermarking Algorithms

Watermarks appeared in the paper industry more than seven hundred years ago to differentiate paper makers¹⁸¹. Since then, they have been extensively used in banknotes and still constitute a very important tool to deter forgery of banknotes¹⁸² — for instance shop cashier in several countries often check the watermark on large bank notes.

In the early nineties, these paper watermarks in banknotes or stamps inspired the first use of the word “watermark” in the context of digital data¹⁸³ and in particular digital images¹⁸⁴. Since then digital watermarking has become a rapidly growing area of research, attracting mainly the signal processing community. Although many topics are still open to further research, a couple of watermarking systems have been implemented in few practical applications, some related to copy control.

¹⁷⁹ Microsoft Research — England.

¹⁸⁰ See: Kirovski, Malvar, Yacobi (2001).

¹⁸¹ See: Kutter, Hartung (1999).

¹⁸² See: Renesse (1998).

¹⁸³ See: Tirkel, Rankin, van Schyndel, Ho, Mee, Osborne (1993).

¹⁸⁴ See: Tanaka, Nakamura, Matsui (1990).

In this context, the audio–visual signal in which data will be hidden is usually referred to as *cover–signal* and the data, that is the sequence of hidden bits, is called the payload. The watermark is the signal which is actually added to the cover–signal so one can refer to its energy. It is obvious that the size of the cover–signal constrains the size of the *payload*: one can hide a larger payload in a 512×512 pixel image than in a single pixel. The *watermark–access–unit* or granularity is the smallest part of cover–signal in which a watermark can be reliably detected and the payload extracted and the *capacity* of the watermarking scheme is bit size of a payload that a watermark–access–unit can carry. In the remaining of this chapter, by *watermarking scheme* we mean the full embedding and extraction algorithms.

Readers who have heard about both watermarking and steganography should not be confused by the two terms as they do represent two very different concepts. Steganography hides the very existence of messages: the hidden information is independent of the cover and should be statistically undetectable. Watermarking adds a payload generally related to the content (e.g., copyright information) and it is usually well known that content is watermarked so the algorithm should be robust to malicious attacks.

Typical requirements for digital watermarking algorithms have been detailed ad nauseam in numerous publications already so we will mention them only briefly here. They include the imperceptibility (or fidelity) of the watermarking process — that is a human listener or viewer should not be able to hear or see whether the cover–signal has been watermarked. The capacity should be high enough for the intended application of the watermarking scheme. The scheme should be reliable (false negative and bit error rates should be low), robust in normal use situations (usually common signal processing), tamper resistant (robust to attacks) and its security should only rely on the secret of keys (following the well known Kerckhoffs’ principles). At last the design of the algorithm will be driven by the cost constraints of the application (number of gates for hardware implementations, speed of the embedding or extraction, etc.).

All these constraints make the design of a watermarking scheme a very challenging task. But over the last decade a basic framework appeared: most watermarking schemes rely on the choice of various basic components that we will describe in the remaining of this section.

I.1 Choice of the Workspace

The watermark casting can be done directly on signal samples¹⁸⁵ or by first applying some transformation such as discrete cosine transform¹⁸⁶, wavelet decomposition¹⁸⁷, Radon transform¹⁸⁸, etc.

¹⁸⁵ See: Pitas (1996); Nikolaidis, Pitas (1998).

¹⁸⁶ See: Barni, Bartolini, Cappellini, Piva (1998).

¹⁸⁷ See: Loo (2002); Kundur, Hatzinakos (1998).

¹⁸⁸ See: Kim, Baek, Lee, Suh (2002).

Fourier transforms enable the embedder to shape the watermark spectrum according to the human perceptual model. For instance Boney et al. propose an audio watermarking scheme where the amplitude of the frequencies of watermark is directly modified with the audio perceptual model derived from the sound track. The modulated complex lapped transform¹⁸⁹ has been used successfully by Kirovski and Malvar¹⁹⁰ in the design of a relatively robust audio watermarking scheme. Wavelets, which have become a powerful tool in image analysis due to their good energy compaction properties and to efficient computation algorithms, have been studied by Loo to watermark images¹⁹¹. More recently, the Radon transform attracted interest because it can be easily used to devise rotation, scale and translation invariant algorithms¹⁹².

I.2 Location of the Watermark

The location of the watermark is usually chosen using some human perceptual model. Audio masking, for instance, is a phenomenon in which one sound interferes with our perception of another sound¹⁹³. Frequency masking occurs when two tones which are close in frequency are played at the same time: the louder tone will mask the quieter one. However this does not occur when the tones are far apart in frequency. Temporal masking occurs when a low-level signal is played immediately before or after a stronger one; after a loud sound stops, it takes a little while before we can hear a weak tone at a nearby frequency. MPEG audio compression techniques¹⁹⁴ exploit these characteristics¹⁹⁵ and Boney et al. have shown that it remains possible to exploit them further by inserting marks that are just above the truncation threshold of MPEG but still below the threshold of perception.¹⁹⁶ Similarly human eyes are less sensitive to noise in area with textures than in smooth areas of images.

Based on these reasons, Cox et al. argued that one ought to embed the watermark in perceptually significant part of the signal/image in the hope that an attacker cannot remove the watermark without causing significant distortions.¹⁹⁷

In addition to the perceptual significance one can also use a key (the seed to a random number generator) to select which coefficients should be modified. Without knowledge of this secret key one should not be able to extract the watermark.

¹⁸⁹ See: Malvar (1998/1999).

¹⁹⁰ See: Kirovski, Malvar (2001).

¹⁹¹ See: Loo (2002).

¹⁹² See: Kim, Baek, Lee, Suh (2002).

¹⁹³ See: Moore (1989).

¹⁹⁴ See: MPEG-2 Audio (1995). A Matlab implementation of the psychoacoustic model is available at: <http://www.cl.cam.ac.uk/~fapp2/software/mpeg/>.

¹⁹⁵ See: Ambikairajah, Davis, Wong (1997).

¹⁹⁶ See: Boney, Tewfik, Hamdy (1996).

¹⁹⁷ See: Cox, Killian, Leighton, Shamoan (1996).

I.3 Encoding of the Payload

A popular way to encode the watermark is to use spread-spectrum techniques. These will be detailed later in this chapter. Error control codes are also often added to the payload before embedding to improve the robustness of the watermark. Although no error correction codes have been specifically designed for watermarking yet, turbo codes have been used by several researchers because their performances are close to Shannon's limit¹⁹⁸ under additive white Gaussian noise.

I.4 Merging of the Watermark with the Cover-Signal

Casting of the watermark, that is the formation of the new signal, is usually done by adding the watermark signal to the host signal but new techniques based on quantisation index modulation have been explored. They quantise the coefficients to be modified instead of simply adding the watermark value. The decoder quantises again the coefficient and looks at which bin each coefficient falls in order to recover the data.

The main difference between the two techniques lies in the exploitation of the knowledge of the cover signal by quantisation based schemes but not by spread-spectrum based schemes. This means that the interference from the cover-signal can be suppressed at the decoder by quantisation based schemes, making detection more reliable in certain circumstances. Both techniques have pro and cons and Chen and Wornell¹⁹⁹ proposed a new solution based on both: the spread transform.

The casting happens in the domain chosen for embedding. For instance Kirovski et al. add a pseudo noise sequence to the frequency coefficient of the modulated complex lapped transform of the signal²⁰⁰ while Ó Ruanaidh et al. modify the phase of the signal²⁰¹.

I.5 Extraction / Detection and Optimisation of the Watermark Receiver

The detection process usually outputs either the recovered payload or some kind of confidence measure indicating how likely it is for a given mark at the input to be present in the signal under inspection.

Private watermarking (also called non-blind watermarking) systems require at least the original cover-signal. One might expect that private schemes will be more robust than the others since they convey very little information and require access to secret material²⁰². *Semi-private watermarking* (or semi-blind watermarking) does not use the original cover-signal for detection but the published

¹⁹⁸ See: Berrou, Glavieux, Titimajshima (1993).

¹⁹⁹ See: Chen, Wornell (2001).

²⁰⁰ See: Kirovski, Malvar (2001).

²⁰¹ See: Ó Ruanaidh, Dowling, Boland (1996).

²⁰² See: Cox, Miller (1997).

watermarked signal²⁰³. The main uses of private and semi-private watermarking seem to be evidence in court to prove ownership and copy control in applications such as D.V.D. where the reader needs to know whether it is allowed to play the content or not. Many of the currently proposed schemes fall in this category²⁰⁴.

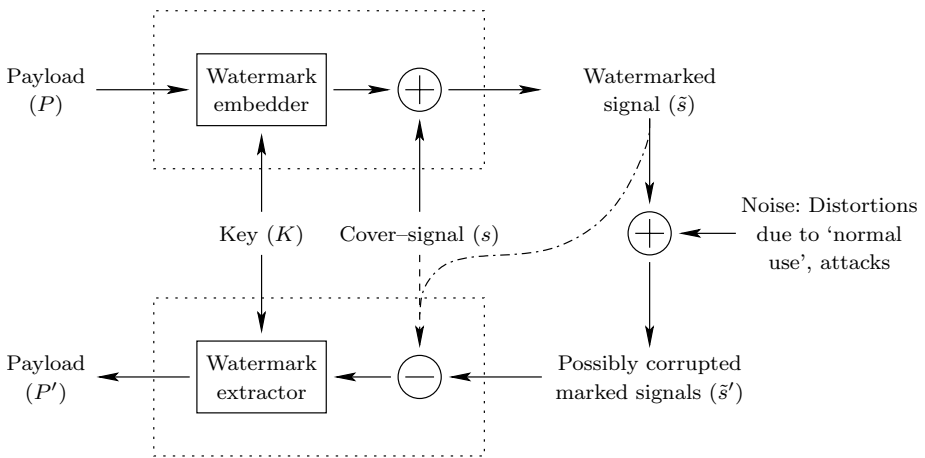


Fig. 1. Basic Model for Digital Watermarking Schemes Showing the Various Inputs of the Embedder and the Optional Inputs of the Extractor.

Public watermarking (or blind watermarking) remains the most challenging problem since it requires neither the secret original nor the published watermark signal. Indeed, such systems really recover the hidden bits (the payload) from the watermarked signal without any additional information²⁰⁵. Public watermarking schemes have much more applications than the others.

There is also asymmetric watermarking (or public key marking) which, like asymmetric cryptographic algorithms, use a different key for embedding and extracting the payload. Very few solutions have been proposed yet²⁰⁶.

For the extraction or detection themselves, most spread-spectrum based watermarking algorithms use correlation as a basis, assuming underlying Gaussian noise interference, for which the correlator is the optimal detector. In practice however, typical audio-visual signals (coefficient in the spatial domain or other transform domain) do not follow the Gaussian model so some authors have been using pre-filtering or other models to improve the detection.

For instance, in the case of audio watermarking it has been noticed that changing the amplitude for watermarking, can make this frequency audible when it

²⁰³ See: Loo (2002).

²⁰⁴ See: Loo (2002); Barni, Bartolini, Cappellini, Piva (1998); Kundur, Hatzinakos (1998); Nicchiotti, Ottaviano (1998); Nikolaidis, Pitas (1998); Tzovaras, Karagiannis, Strintzis (1998); van Schyndel, Tirkel, Osborne (1994).

²⁰⁵ See: Kirovski, Malvar (2001); Swanson, Zu, Tewfik (1996); Langelaar, van der Lubbe, Lagendijk (1997); Zhao, Koch (1995); Dugelay, Roche (1999).

²⁰⁶ See: Kirovski, Malvar, Yacobi (2001).

was not or vice versa. This leads to an imbalance between negative and positive components of the watermark which can have dramatic effect on the efficiency of the detection. Modified covariance test appear to be a good solution²⁰⁷.

II Basics of Digital Watermarking

One very popular way to watermark multimedia content uses spread-spectrum encoding and correlation based extraction.

General spread spectrum systems encode data in the choice of a binary sequence that appears like noise to an outsider but which a legitimate receiver, furnished with an appropriate key, can recognise. Spread-spectrum radio techniques have been developed for military applications since the mid-1940's because of their anti-jamming and low-probability-of-intercept properties²⁰⁸; they allow the reception of radio signals that are over hundred times weaker than the atmospheric background noise.

Tirkel et al.²⁰⁹ were the first to note that spread-spectrum techniques could be applied to digital watermarking and later a number of researchers have developed watermarking techniques based on spread-spectrum ideas which take advantage of the large bandwidth of the cover medium (image, sound, video) by matching the narrow bandwidth of the embedded data to it.

As noticed earlier, high frequencies can be used to ensure imperceptibility of the watermark but are inadequate as far as robustness is concerned, whereas low frequencies are of interest to ensure robustness but have limited use because of the unacceptable impact on the quality of the signal after watermarking. Spread spectrum can reconcile these conflicting points by allowing a low-energy signal to be embedded in each one of the frequency bands.

Direct-sequence spread-spectrum simply adds a pseudo random sequence to the signal and detection can be achieved using a simple correlator. As mentioned earlier this assumes a Gaussian model and this also requires perfect synchronisation between the transmitter and the receiver.

In combination with perceptual models spread-spectrum based watermarking schemes usually survive most basic signal processing attacks. In the next section we will see how they can be improved to survive some amount of desynchronisation.

II.1 Improving the Robustness of Basic Algorithms

Basic watermarking algorithms such as the spread-spectrum techniques briefly presented in the previous section or such as the recently hyped quantisation index modulation techniques are all prone to some form of desynchronisation attacks. In fact the basic algorithms themselves assume prior synchronisation. Algorithms

²⁰⁷ See: Kirovski, Malvar (2001).

²⁰⁸ See: Pickholtz, Schilling, Milstein (1982).

²⁰⁹ See: Tirkel, Rankin, van Schyndel, Ho, Mee, Osborne (1993).

for practical application need to be able to perform this synchronisation though. In the case of images for instance rotation, scaling and translation are a very easy way to achieve this.

One general idea is to embed the watermark in a space which remains invariant to the expected transformations. So for instance, the Fourier Mellin transform or the Radon transform are both invariant to rotation, scaling and translation. They have been used successfully to embed watermarks which are robust to these transformations²¹⁰.

Another idea is to embed two watermarks: a reference watermark (or template) and the actual watermark which carries the payload. Unfortunately this has an obvious drawback: an attacker just needs to focus on the template and try to remove it.

For small distortions simple redundancy of the watermark can be used²¹¹: rather than doing the correlation test using each sample of the random spreading sequence, each sample is repeated and the correlation is done only at the centre of the repeated zones. So as long as there is a certain overlap between the detection zone and the original embedding zone, detection can be done accurately.

Many other tricks are used. In fact over the last decade watermarking algorithms have improved a lot and become robust to a growing number of attacks. Herley²¹² argues that “this has created an illusion of progress, when in reality there is none” because “algorithms protect all objects in a neighbourhood surrounding the marked object; [...] while this is necessary it is very far from being sufficient”. Another reason is that people have come up with attacks faster than counter-attacks! So in the next section we will look at some unresolved problems which seriously undermine the reliability of watermarking technologies.

III Attacks

If breaking a single player does not pose a security threat, the main target of the adversary is finding a signal processing primitive that removes the watermark or prevents a detector to find it: a successful attack is achieved either when the watermark is removed or when the watermark detector is fooled.

Several attack mechanisms have been largely successful in setting up robustness benchmarks for watermarking technologies. In fact, as soon as people have tried to develop watermarking technologies, others have attempted to break them. The Oracle attack or the estimation-based attack fall into the first category; while attacks such as desynchronisation or blind pattern matching attack, fall into the second. These attacks will now be described briefly.

²¹⁰ See: Kim, Baek, Lee, Suh (2002).

²¹¹ See: Kirovski, Malvar (2001).

²¹² See: Herley (2002).

III.1 Removal

The estimation or removal attacks usually try to estimate the original non-watermarked cover–signal, considering the watermark as noise with given statistic. For instance, Langelaar et al.²¹³ showed that 3×3 median filtering gives a good approximation of original pictures in the case they have been watermarked using spread–spectrum. So far, estimate–and–remove attacks have introduced fairly strong blurring effects but recent work based on maximum a posteriori watermark estimation and re–modulation has given promising results²¹⁴.

In the case of transaction watermarking (often called fingerprinting²¹⁵), another way to remove the watermark is to use copies from different sources and mix them (either by averaging them or concatenating pieces of them like a mosaic attack²¹⁶) to generate an un–watermarked copy. These are usually referred to as collusion attacks²¹⁷.

III.2 Oracle

The idea of the Oracle (or sensitivity attack)²¹⁸ is to explore, pixel by pixel, an image at the boundary where the detector changes from “mark absent” to “mark present” and iteratively construct an acceptable image in which the mark is not detected. Of course, with a programmable tamper–proof processor, one can limit the number of variants of a given picture for which an answer will be given, and the same holds for a central mark reading service. But in the absence of physically protected state, it is unclear how this attack can be blocked. In most applications an attacker has access to a detector. This detector can be a piece of software shipped with a major image processing package or an electronic circuit embedded into consumer electronics such as D.V.D. Even if the attacker does not know much about the watermark embedding method, he can still use the information returned by the detector to remove the watermark by applying small changes to the image until the decoder cannot find it anymore.

The attacker starts by constructing an image that is very close to the decision threshold of the detector (see Fig. 3): modifying this image very slightly should make the detector switch from “watermark present” to “watermark absent” with probability close to 0.5. Note that the constructed image does not need to resemble to the original. This can be achieved by slightly blurring repeatedly the image until the detector fails to find a watermark, or by replacing progressively pixels by grey.

²¹³ See: Langelaar, Lagendijk, Biemond (1998).

²¹⁴ See: Voloshynovskiy, Pereira, Herrigel, Baumgartner, Pun (2000); Kutter, Voloshynovskiy, Herrigel (2000).

²¹⁵ Not to be confused with the content-based identification technologies also called fingerprinting, see: *Herre* within this book on page 93.

²¹⁶ See: Petitcolas, Anderson, Kuhn (1998).

²¹⁷ See: Cohen, Zemor (1994); Boneh, Shaw (1998).

²¹⁸ See: Linnartz, van Dijk (1998).

The second step analyses the sensitivity of the detector to modification of each pixel. The luminance of a given pixel is increased or decreased until the detector changes its output. This is repeated for each pixel. From this analysis the attacker can divide a combination of pixels and modifications such that the distortions in the image are minimised and the effect of the modifications on the detector are maximised, that is that the watermark is not detected.

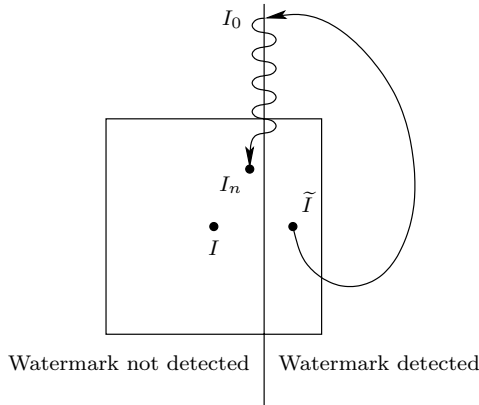


Fig. 2. The plan of the page corresponds to all possible images, I is the original image and \tilde{I} the image with watermark. The square contains all images that look similar to I . The attacker uses \tilde{I} and starts by constructing an image I_0 that is very close to the decision threshold of the detector. The luminance of a given pixel is increased or decreased until the detector changes its output. This is repeated for each pixel until an image I_n , perceptually closed to \tilde{I} but where no watermark can be detected, is created.

III.3 Stirmark

Stirmark is one of the oldest attacks against image watermarking algorithms. It uses a fact we mentioned earlier: most watermarking detection or extraction algorithms have to perform some correlation which is very sensitive to synchronisation. Stirmark achieves desynchronisation by introducing small random distortions.

These small random geometric distortions can also be applied to video, provided that the random parameters are saved; otherwise a wobbling effect appears when the video is played.

Since it was first written in 1997, Stirmark has been improved a lot becoming the first benchmark suite and later the first online watermarking evaluation service²¹⁹. So not only it includes the simple and powerful attack described above but also a large set of other attacks that can be tuned by the user depending on the application and type of watermarking technique to be tested.

²¹⁹ See: Petitcolas (2000); Petitcolas et al. (2001).

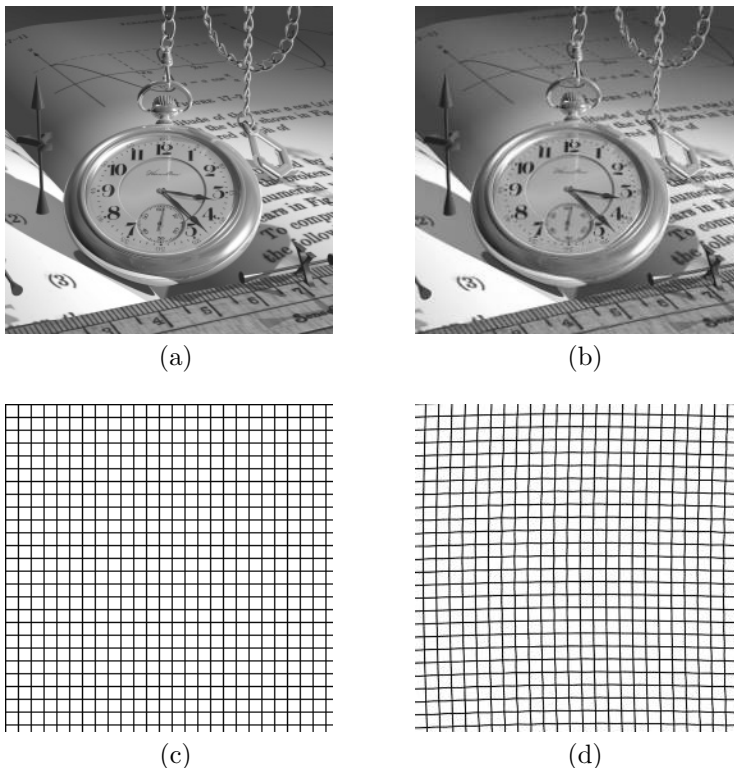


Fig. 3. When applied to images, the distortions introduced by Stirmark are almost unnoticeable: watch before (a) and after (b) Stirmark with default parameters. For comparison, the same distortions have been applied to a grid (c & d).²²⁰

III.4 Blind Pattern Matching

The blind pattern matching attack²²¹ permutes block of audio which sound similar to the human listener. In most cases these blocks will contain different watermarks or different part of the same watermark and the permutation has the effect that watermark cannot be detected anymore. The attack consists in three main steps. First the signal is partitioned into small overlapping blocks. Then perceptually similar blocks are identified — this similarity can either be direct or modulo some simple transformations (e.g., time stretching and amplitude scaling). Once the similar blocks are identified they are permuted; this permutation has very small effect on the general perceptual quality of the signal because permuted blocks were chosen such that they sound the same or they look the same.

²²⁰ *Pocket Watch on a Gold Chain*. Copyright image courtesy of Kevin Odhner (jko@home.com)

²²¹ See: Petitcolas, Kirovski (2002).

The blind pattern matching attack is not limited to a type of content or to a particular watermarking algorithm. For example, systems that modulate secrets using spread-spectrum and/or quantisation index modulation are all prone to the blind pattern matching attack. In order to launch the attack successfully, the adversary does not need to know the details of the watermark algorithm. The adversary needs to reduce the granularity of integral blocks of data such that no block contains enough information from which a watermark can be identified individually.

Note that watermark detection involves processing large amount of data (for example, reliable and robust detection of audio watermarks requires at least several seconds of audio). Thus, blocks considered for blind pattern matching must be at least one order of magnitude smaller than watermark length. For both audio and video, this requirement is not difficult to satisfy as typically blocks of 128–1024 transform coefficients for audio or bitmaps of up to 64×64 pixels for video are considered for pattern matching.

Finding a counter-measure to this type of attack remains an unsolved problem as one can exchange similar blocks between two different signals — so one could find similar block between a piece of Schubert and another one of Eminem. The search space becomes so large that any counter-measure trying to analyse possible permutations during the embedding process becomes computationally infeasible.

IV Concluding Remarks

The *illusion of progress* created by the vast amount of research done in the watermarking area amplified by the excitement surrounding any new research field, hides fundamental security issues which remain unresolved. Serious misunderstandings between designers and “users”, serious misalignments between expectations and hype in the media make the situation worse.

The nearly four hundred years old battle between content owners and consumers²²² is not likely to be solved in the near future. Some have suggested that only a change of business model is the answer to the problem²²³.

This solution is probably extreme and careful design of digital rights management systems might help improving the situation; watermarking however does

²²² Claude Gellée of Lorraine (1600–1682), also known as Claude Lorrain, was a landscape painter whose reputation was such, that he was attracting imitations. So he introduced a method for protecting his work nearly hundred years before any relevant law was created. From some time around 1635 until the end of his life in 1682, Lorrain kept a book that he called the *Liber Veritatis*. The Liber was a collection of drawings in the form of a sketchbook, which contained around 195 drawings. According to some historians, any comparison between drawings and paintings goes to show that the former were designed to serve as a “check” on the latter and from the Liber any very careful observer could tell whether a given painting was a forgery or not.

²²³ See: Fox (1999).

not seem to raise the barrier very much against pirates. It has only a small role to play in the wide area of digital rights management systems and may end up being used in niche markets only. Indeed watermarking algorithms have been far easier to break than most copy protection mechanisms based on tamper resistant hardware and one can rightfully question their reliability for such sensitive applications.

2.3.4 Content Based Identification (Fingerprinting)

Jürgen Herre²²⁴

I Introduction

Ever since the broad availability of efficient source coding methods (data reduction) and digital distribution channels (including the Internet), consumers have seamless access to an enormous amount of multimedia data. This includes audio material and still and moving pictures within a wide range of quality, ranging from “pre-view” (e.g. Internet radio) to broadcast quality. As a result, efficient handling of this considerable amount of data has become a challenge of its own (e.g. “how can I find desired material efficiently?”). This has led to the definition of a number of so-called *metadata* standards. Examples for such specifications include the Dublin Core initiative²²⁵, the SMPTE/EBU Dynamic Metadata Dictionary²²⁶, the P/Meta project of the European Broadcasting Union (EBU)²²⁷ and, more recently, the MPEG-7 standard²²⁸. The general idea behind these standards is to define data formats which provide a comprehensive description of the actual multimedia content in an interoperable way. Such meta-data (i.e. “data about data”) structures may include a wide range of descriptions of the origin and identity of the content, its structure, usage rules, and various perceptual or semantic aspects.

Among the many conceivable ways of characterizing a piece of audiovisual content, the unique description of the content identity based on its signal representation (so-called “content-based identification”) is of great importance. This functionality is frequently also referred to as *fingerprinting*²²⁹ and enables automatic identification (including title, author and other description of the works) of content which has been registered previously in an internal database of reference data. The topic of fingerprinting has received much attention recently in both research and commercial deployment and current technological development has shown that, depending on the underlying technology, reliable and efficient identification can still be achieved even for distorted input signals and large databases of multimedia material.

This article discusses the concept of content-based identification and the underlying technological challenges as well as some of its many attractive applications

²²⁴ Fraunhofer Institut für Integrierte Schaltungen, Erlangen, Germany.

²²⁵ Web site of the Dublin Core Metadata Initiative: <http://dublincore.org/>

²²⁶ See: SMPTE (2001).

²²⁷ See: Hopper (2000).

²²⁸ See: MPEG-7 Introduction (2001).

²²⁹ As a note to the reader it should be mentioned that the term *fingerprinting* is occasionally also used in the literature in the context of digital watermarking where the idea is to enable unambiguous identification of the content by imprinting a unique mark into the signal (rather than deriving a fingerprint from it). Unfortunately, this use of terminology may lead to considerable confusion and is, therefore, not endorsed by the author.

in the multimedia area. Owing to the underlying idea, the fingerprinting approach is very different in its nature from (and in fact in a sense complementary to) the concept of watermarking. Thus, the article is concluded by contrasting both approaches with respect to their use cases.

II The Concept of Fingerprinting

During the recent years, a number of technologies for fingerprinting of multimedia material were developed. In contrast to the identification of content based on embedded digital watermarks, fingerprinting is a “non-invasive” approach which does not require any modification of the original multimedia signal. The underlying idea consists of identifying the audio/image/video content directly by examining the characteristics of its signal representation using a *pattern recognition* process. As usual within the framework of pattern recognition, a *training phase* is required so that the characteristics of the items to be recognised are introduced into the system. This leads to a two-stage process (see Figure 1):

- During the *training phase*, characteristic features are extracted from a set of known reference items such that the extracted feature data forms a unique combination which allows for the unambiguous distinction of a particular item from all other entries. Such feature representations can be made extremely compact (e.g. several orders of magnitude smaller than MP3-compressed audio) and are frequently called *fingerprints*, *signatures*²³⁰ or *robust hashes*²³¹. For each item which should be recognised later by the system, such a fingerprint is generated and stored in a reference database together with some of its descriptive metadata. This metadata may be just enough for the identification of the individual item in terms of bibliographic reference (e.g. title name, artist) or may contain richer descriptions of the content.
- During the *recognition phase*, the signal to be identified (*query* item) is presented to the system and used for the extraction of a fingerprint in a way similar to that of the training phase. The actual recognition process is based on comparing this query fingerprint with the fingerprints that are stored in the reference database. The most “similar” fingerprint found in the database corresponds to the best matching (and most likely) reference item. As a result of this comparison process, the system delivers an indication of whether the presented signal has been successfully identified and, if this is the case, the database ID of the identified item together with a measure of the achieved recognition confidence. Furthermore, the metadata associated with this database item may be returned by the system.

²³⁰ See: Hellmuth, Allamanche, Herre, Kastner, Cremer, Hirsch (2001).

²³¹ See: Haitisma, Kalker, Oostveen (2001).

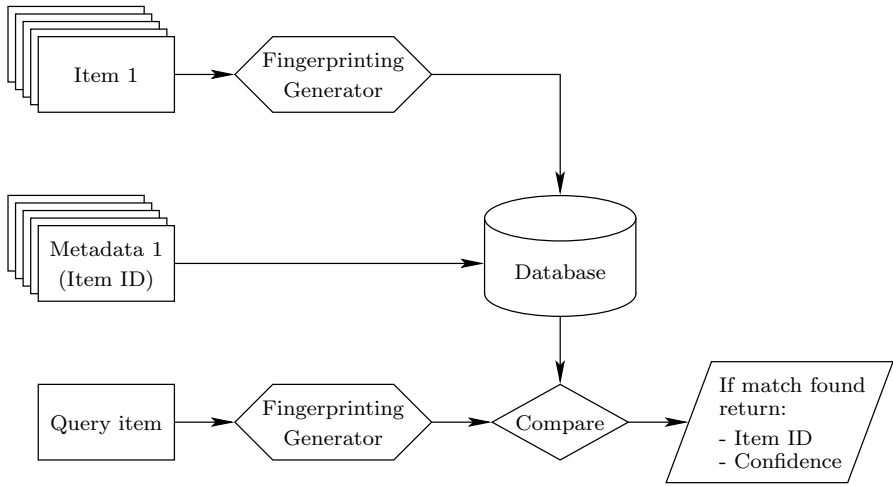


Fig. 1. Generic Structure of a Fingerprinting-based System for Content Identification

A good fingerprinting system should satisfy a number of requirements. The most important of them are briefly discussed here:

- *Robustness*: When content-based recognition schemes are used in real world application scenarios, it is essential that correct identification is maintained also in response to a distorted query signal which is comparable to the requirement of robustness in the watermarking context. As an example, audio signals may have undergone simple modifications (such as level change, linear filtering/equalisation, bandwidth limitation, noise addition) or more complex alterations (such as MP3 data compression, GSM speech coding, watermarking, pitch and speed change). Furthermore, identification should also be possible if only arbitrary parts of the full signal are presented to the recognition engine (e.g. “15 seconds of audio starting at 1 minute 20 seconds into the song”) in a way analogous with the human ability of recognising excerpts. Finally, the system is required to reliably reject unknown content rather than confusing it with any of the registered reference items.
- *Signature compactness*: Considering the fact that some applications of fingerprinting require recognition ability for millions of content items and that the system has to handle the corresponding amount of signature information, it becomes clear that the *compactness* of the signatures is of great importance. After the feature extraction process, only an extremely small fraction of the original information is retained. The signature data rates are usually several orders of magnitude lower than the rates used for audiovisual source compression since reconstruction of a representation in the original audiovisual domain is not intended. Nonetheless, this fraction of data has to support a reliable distinction between the query item and all other items in the reference database.

- *Search Speed*: As an additional requirement, the search process must be completed within a time period that is acceptable in the context of the application even for large search spaces (i.e. large signature databases).
- *Speed of signature extraction*: For the creation of comprehensive signature databases (e.g. several million items) from available audiovisual material, a fast signature extraction process is of major importance in order to complete the task within a realistic time frame. As an example, for many audio fingerprinting applications an extraction time that is significantly below the playing time of the item may be desired.

As is known to be true for many technologies, not all desired performance parameters of a system can be optimised independently. In the field of fingerprinting, a dependency between the recognition robustness and the compactness of the signatures can be observed²³². Usually, high robustness with respect to signal distortions can be achieved only by accepting an increased signature datarate. Conversely, applications which deal only with slightly distorted signals permit usage of extremely compact signature formats. It is instructive to compare this two-way trade-off to the three-way dependency between robustness, datarate and perceptual transparency that has been formulated in the watermarking context²³³.

From the principles discussed so far it becomes clear that fingerprinting-based systems achieve an identification of query signals based on their *similarity* with respect to the items contained in a reference database (*similarity-based* matching). It is mainly the type of features employed for signature extraction which determines what is interpreted as similarity by the system and thus plays a crucial role in the performance of the system. Depending on the nature of input signals, a large number of different features have been used for this purpose, such as color/shape/motion for video input, and spectral/temporal characteristics for audio signals. As fingerprinting systems are typically optimised for the best possible distinction between several items and reliable recognition even in the context of signal distortions, items that appear similar to a human observer (in whatever sense) are typically classified as “dissimilar” by such systems. Examples from the area of audio fingerprinting are:

- A “known” music title which is performed by a different artist,
- A person singing or humming the title’s melody or
- A different performance (e.g. “live version”) even by the original artist.

Thus, it is important to understand that such systems are generally *not* optimised to model subjective similarity of content, but to achieve a reliable distinction between different content even though it may be considered similar by humans. This approach is in fact a necessary requirement for enabling identification of different artistic instantiations of the same theme.

²³² See: Kastner, Allamanche, Herre, Cremer, Grossmann, Hellmuth (2002).

²³³ See: Neubauer, Herre (2000).

III An Example: MPEG-7 Audio Fingerprinting

The increasing interest recently in content-based identification has also stimulated a number of publications and systems in the area of audio fingerprinting which try to establish a presence in the market place, e.g.²³⁴. For the vast majority of these systems a comprehensive description of the underlying technological foundations is not available in view of their commercial background. Therefore, this section will illustrate the concept of audio fingerprinting by examining a current development based on the recent MPEG-7 Audio standard²³⁵. Owing to the standard-based approach, this technology relies on a fully specified open format of the signature data²³⁶.

- *Signature features*: The system relies on the so-called *spectral flatness* (SFM)²³⁷ of the audio signal which is calculated within subbands of 1/4 octave width each. Roughly speaking, this feature relates to the presence of tonal components within the subbands. The signature contains SFM data for a user selectable number (at least 4) of subbands starting at a frequency of 250Hz.
- *Computational complexity*: An extremely fast signature extraction process can be achieved by using current Personal Computers (ca. 100 times faster than the actual playing time of the music title). The recognition part can be implemented efficiently on both general purpose computing platforms (PCs) as well as portable devices, such as Personal Digital Assistants (PDAs).
- *Recognition performance*: The system is robust to common signal distortions and is able to identify arbitrary excerpts of the query item independent of its temporal offset. For a test database of 85.000 music titles and a number of signal distortions, a recognition performance of typically better than 99.7% was achieved.
- *Scalability*: Different fingerprinting application scenarios are usually associated with different robustness requirements and, thus, different optimal “operating points” in the trade-off between the compactness of the signature and its robustness. Using MPEG-7 Audio signatures, this can be accounted for by *scaling* several parameters of the signature in response to the application requirements and thus controlling the recognition strength (and, thereby also, the data rate). In this way, a range of signature data rates between 2

²³⁴ See: Auditude web site: <http://www.auditude.com>; Wold, Blum, Keislar, Wheaton (1996); etantrum music id. web site: <http://www.etantrum.com>; Haitisma, Kalker, Oostveen (2001); Kurth, Clausen (2001); Neuschmied, Mayer, Battle (2001); Moodlogic Inc. web site: <http://www.moodlogic.com>; Relatable web site: <http://www.relatable.com>; Shazam Entertainment Ltd. web site: <http://www.shazam.tv>; Tuneprint (robust psychoacoustic fingerprinting) web site: <http://www.tuneprint.com>.

²³⁵ See: MPEG-7 (2001); Lindsay, Herre (2001).

²³⁶ See: Allamanche, Herre, Hellmuth, Fröba, Cremer (2001); Hellmuth, Allamanche, Herre, Kastner, Cremer, Hirsch (2001); Kastner, Allamanche, Herre, Cremer, Grossmann, Hellmuth (2002).

²³⁷ See: Jayant, Noll (1984).

Bytes/s und 800 Bytes/s is covered, the default setting corresponding to a rate of approximately 32 Bytes/s. Furthermore, “richer” signatures can be transcoded into “lighter” and more compact signature formats, thus enabling a meaningful comparison between signatures that have been parameterised differently. This *scalability* property permits a high degree of flexibility so that very different requirements can also be satisfied by the same generic data format²³⁸.

IV Applications of Fingerprinting Technology

In the current and future world of multimedia, automatic recognition of content by means of fingerprinting technology has a plethora of attractive applications, some of which are briefly illustrated here:

- *Identification of content and finding associated metadata*: Naturally, fingerprinting technology allows to easily handle unknown audiovisual content (which is *not* annotated by descriptive information) by determining its identity and finding associated metadata. This is an extremely interesting property when trying to benefit from metadata-based services for today’s non-annotated legacy content (such as Compact Discs, VHS video tapes) and works regardless of the kind of media on which the content resides. Note that metadata might also include information on the usage policy associated with a certain piece of audiovisual content.
- *Music sales*: Using this technology, consumers can identify — and possibly order on the spot — interesting content they observed in whatever situation by pressing the identification button on their electronic device. Identification may be performed on PDAs, PCs or via mobile phone.
- *Protection of content-based intellectual property*: Fingerprinting may be employed to find out if and where illegitimate/pirated content is located on the Internet. This is achieved by combining a fingerprinting-based recognition engine with a “web crawler” process which examines the Internet for content and feeds the results through the recognition engine. As a result, a list of “what was found where” can be automatically compiled and used to take-down illicit content.
- *Broadcast monitoring*: Similarly, fingerprinting based systems may be used to implement automated “24 hours per day, 7 days per week” monitoring and analysis of transmitted broadcast programme material. The results can be used e.g. for purposes of media research or simply to verify the accurate transmission of customer’s advertisement spots. Furthermore, analysis of the recovered programme data (“how often was a song/video was played?”) may be utilised to ensure proper compensation of the rights holders for the transmitted content. This type of use has been among the first and very early applications of fingerprinting.

²³⁸ See: Kastner, Allamanche, Herre, Cremer, Grossmann, Hellmuth (2002).

V Digital Watermarking versus Fingerprinting

As can be seen from the previous discussion of the principles of fingerprinting, this technology uses an approach which is clearly different from the one employed by digital watermarking. The following section gives a brief synopsis of the essential characteristics of both types of technologies when used for the purpose of automatic identification of content.

A first obvious reason for the different characteristics of both approaches is rooted in the fact that the process of watermarking implies embedding an information-bearing signal into the content while this is not the case for fingerprinting. This has a number of consequences with respect to the applicability of both technologies to certain usage scenarios:

- In order to employ watermarks it is essential to have access to the content *prior to* its distribution in order to perform the embedding operation. This is not required for the use of fingerprinting-based technology. Consequently, the latter type of technology is also applicable to “legacy content” which has been published before in traditional formats (e.g. Compact Discs or VHS tapes).
- On the other hand, watermarking enables the individual marking of multiple copies of the same works, such that, e.g., it becomes feasible to recover the information on which customer a particular copy was sold to. Fingerprinting-based systems do not provide the capability for such a distinction.
- While watermarking technology always carries a certain risk of introducing perceptual degradations into the content, no such risk exists for a fingerprinting-based approach.
- If it is found desirable at some point to upgrade to a new watermarking scheme with better performance parameters (e.g. higher data rate, robustness or perceptual quality), it is necessary to re-process the entire content database with the upgraded technology and re-distribute the result. An upgrade to an improved fingerprinting system, in contrast, does not require such an effort and may thus be much easier to accommodate.
- In return, watermarking does not require any change of the “receiver” (detector) side if new content items should be included into a service. In the case of fingerprinting, the recognition engine has to be trained to enable detection of the additional content.
- While watermarking does not exhibit a dependency of the computational effort for content identification on the number of different content items to be recognised, the effort for fingerprinting generally increases with the size of the signature database due to the increased search space. (No reference database is needed in the case of watermarking.)

In light of these observations, both approaches show complementary characteristics which can supplement each other very well, depending on the desired application scenario.

VI Conclusions

The concept of automated content-based identification of audiovisual material has received widespread interest recently due to the enormous growth in the amount of available material to everyone and the necessity of efficient handling of such material. The underlying idea for this technology is to perform a similarity search between the unknown (query) item and items stored in a reference database by comparing their condensed representations (fingerprints). The resulting approach for content identification shows properties that are different from — and mostly complementary to — the characteristics of digital watermarking. Both technologies enable a considerable number of very attractive applications in the area of digital rights management and beyond.

2.3.5 Rights Expression Languages

*Susanne Guth*²³⁹

Abstract: This chapter provides an overview of the field of rights expression languages (RELS). It justifies the need for rights expression languages in today's DRM systems and addresses the requirements which have to be met by these languages. An REL is basically a means of expressing the rights of a party to certain assets. Therefore, all rights languages have a similar basic language concept, which is also introduced in this chapter. Standardization is a critical success factor for RELS, thus all important standards and other initiatives are briefly described as well. The chapter also deals with current and potential fields of application for RELS, after which two practical examples (XML instances) of rights languages are presented. Finally, the chapter gives an overview of the current market situation and trends in the field of DRM middleware and implementations using RELS.

I Introduction

The number of online marketplaces has grown steadily in recent years²⁴⁰ and will continue to expand in the future. Wherever commercial goods are exchanged electronically, there is a need for contracts to specify the terms and conditions of the transaction. Most of the resulting contracts are stored in digital format. Digital contracts are exchanged among different information systems for various reasons: to fulfill the contract (i.e., to exercise the rights granted), to pay the amount agreed upon, to rescind the contract and so on. Digitally signed contracts are legally binding²⁴¹. They are also of public interest and have to be readable for third parties.

However, in other non-commercial fields of application for digital contracts, a monetary consideration might not be part of the agreement for a digital good, for example in education. Authors of learning materials might be more interested in a good reputation than in revenues. Nonetheless, they may still wish to restrict access and usage rights to their materials in order to prevent modification or re-distribution. The two cases mentioned describe situations in which rights information is specified in the form of contracts. The contracts state the rights and relationships of the contracting parties to the subject matter of the contract.

The need to express rights is not solely desired for the purpose of formulating contracts. In the private domain, Internet users demand discreet handling of their personal data. They wish to have a guarantee that their personal information is accessible only in compliance with data privacy laws or in accordance with additional rights which they grant personally.

A number of organizations and companies have recognized the need for a standard rights expression language (REL) which has the power to express usage

²³⁹ Vienna University of Economics and Business Administration.

²⁴⁰ See: Johnson (2002).

²⁴¹ See: E-SIGN. Directive (1999).

and access rights and supports the applications mentioned above. Accordingly, a rights expression language has to support the implementation of frameworks which enable the interoperability of DRM systems and agents on the basis of digital contracts (or digital documents).

II Requirements for Rights Expression Languages

A rights expression language provides a means of expressing use and access rights to assets. It should be sufficiently rich to formulate business models and to express terms and conditions for digital publications, audio and video files, images, games, software, and other digital assets, regardless of whether a monetary consideration is part of the transaction. The application of a standardized REL facilitates interoperability and consistency among DRM systems, which manage the creation, controlled distribution and consumption of digital or physical goods and services.

In order to provide the above-mentioned functionality, an REL must fulfill a number of technical and conceptual requirements. One substantial technical requirement for RELs is machine readability. Therefore, all of today's RELs have chosen serialization in XML. XML documents are machine readable and interpretable and thus qualify as an exchange format for digital documents. Stating rights information in an XML-based language allows flexible expressions, as the expression elements are not restricted to the columns of a relational database table.

The following activities might be involved in managing the consumption of digital goods: the authentication of the consumer, verifying the consumer's rights on the basis of his/her role or identity, granting or denying access, decrypting and decompressing digital goods, rendering the digital goods according to the permissions granted, notifying the content provider of the consumption, calculating royalties for the provider or other involved parties, and processing payments.

A number of REL requirements can be derived from the example given. In order to provide the relevant metadata, the REL should support the articulation of roles, standard identification systems (such as DOI²⁴², ISBN, ISSN etc.), the definition of usage permissions and their restrictions (or prerequisites), the expression of revenue and payment details, security information, details on technical handling (decryption algorithms, viewers, media format) as well as workflow data.

This informal enumeration does not represent a complete list of requirements for an REL. The Moving Pictures Expert Group (MPEG) (see page 106) has formally specified the requirements for a rights expression language and its rights data dictionary for the multimedia domain²⁴³. The document defines additional requirements such as concepts for content aggregation, permissions and parties,

²⁴² See: *Paskin* within this book on page 26.

²⁴³ See: MPEG-21 Requirements (2002).

the sequencing of elements, etc. The requirements of a rights language vary depending on their field of application and scope, thus the REL should be open and extensible.

III Components of a Rights Expression Language

The two constitutive factors in a language are its syntax and semantics. The term ‘syntax’ refers to the grammar rules which apply to the language’s vocabulary, whereas the term ‘semantics’ refers to the meaning of valid “sentences” in the language. For the purposes of this chapter, the grammar of RELs is referred to as the *rights language concept*, and the semantics of rights vocabulary are defined by the *rights data dictionary (RDD)*. A valid sentence in an REL is called a rights expression or an REL instance. Rights expression languages have the power to express the rights of parties to particular assets. Thus RELs have the power to formulate simple stand-alone rights expressions as well as complex digital contracts.

III.1 Rights Language Concept

The most basic elements in every rights language concept are rights, assets and parties²⁴⁴; the names of these three basic elements vary in each REL.

- *Rights* are understood as expressions which grant certain usage or access permissions to digital goods or services. Permissions can be specified in more detail as prerequisites or restrictions. Prerequisites describe terms or duties that have to be fulfilled before a right is granted. Restrictions serve to narrow the right granted, for example by time, location, individual etc.
- The *asset* represents the digital good or service to which the rights apply. The asset has to be described by a non-ambiguous identifier such as a DOI²⁴⁵).
- The *party* element represents any kind of party, be it a legal entity or physical person, which has a relationship to a digital product or service. In contracts, the party elements predominantly represent the people who enter into the contract. Examples of parties include the rights holder, author, creator, content provider, consumer, administrator and the like.

Starting from this basic model, each REL contains additional concepts for the purpose of expressing rights relationships in more detail, for example by means of prerequisites and restrictions on permissions. The paragraphs that follow present an example of a language concept: the straightforward concept of the Open Digital Rights Language (ODRL) (see page 105).

The root element in ODRL is the *rights* element, which represents one rights expression (e.g., a license, contract, etc.). The rights element may contain the rights expression itself with the *party*, *asset* and *permissions* elements or, alternatively, it may use the *offer/agreement* element to indicate semantically that

²⁴⁴ See: Iannella (2001).

²⁴⁵ See: Paskin within this book on page 26.

a given rights expression is an offer or agreement. In ODRL, prerequisites are called *requirements*, and restrictions are called *constraints*. ODRL also provides for *conditions*. Once a condition is fulfilled, the right is revoked.

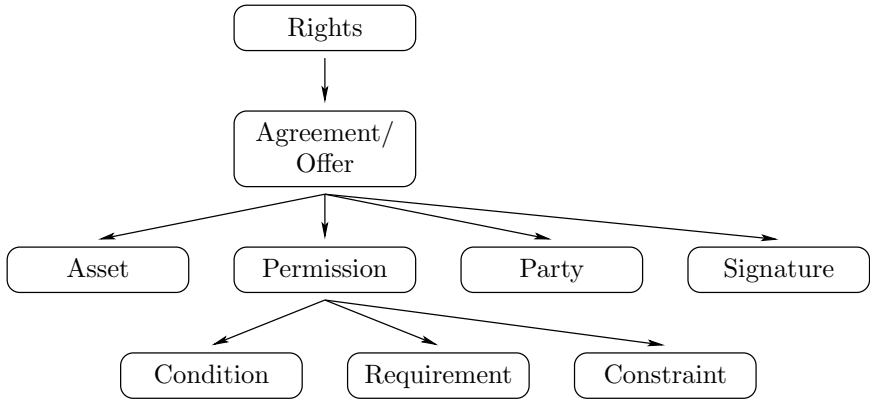


Fig. 1. A Subset of the ODRL Language Concept

If the ODRL rights expression includes a digital signature, the corresponding information can be expressed by means of the *signature* element. The ODRL language concept allows the addition of XML elements compliant with the XML Signature²⁴⁶ namespace. Figure 1 illustrates the elements discussed, which are merely a subset of the ODRL language concept. For a full description of the concept, please refer to Iannella²⁴⁷.

All ODRL elements can be further described by means of an ID, name, etc. with the help of the *context* element (not shown in Figure 1).

A rights expression can specify multiple parties, multiple or bundled assets as well as multiple permissions. Each permission can have prerequisites and constraints. In the next section, we will look at the rights vocabulary provided in order to create instances of this language concept.

III.2 Rights Data Dictionary (RDD)

Each rights expression language includes a rights vocabulary, which defines the vocabulary permitted and its semantics in REL instances (i.e., valid rights expressions). For example, in an REL instance the print, play or view vocabulary items may be used as granted permissions; the time, location and individual vocabulary items may be used to restrict the permissions granted; or the payment vocabulary item may be used to express a requirement to obtain a permission. The table below shows an extract from the ODRL rights data dictionary in which several permission elements are defined.

²⁴⁶ See: Bartel (2002).

²⁴⁷ See: Iannella (2002).

Name	Identifier	Description	Comment
Play	play	The act of rendering the asset in audio/video form.	...
Print	print	The act of rendering the asset on paper or hard copy form.	...
Execute	execute	The act of executing the asset.	...
...			

Similar vocabulary definitions exist for requirements, constraints and the context element. The condition element can be expressed by means of the requirements and constraints vocabulary. A valid instance in the language concept and vocabulary introduced here can be found on page 109.

The rights data dictionary of the indecs 2rdd project (see page 106) aims to provide a more sophisticated RDD than one that simply defines vocabulary. The project has also provided an approach to a rights ontology which supports the interoperability of various rights metadata models.

IV Standards and Initiatives

In this chapter, we introduce the relevant standards in the field of rights expression languages. The field is still evolving, but the standards mentioned below have managed to prevail.

IV.1 ODRL

The Open Digital Rights Language (ODRL)²⁴⁸ is being developed by the ODRL initiative²⁴⁹. The ODRL initiative is an international effort which aims to develop an open REL standard for the DRM sector. In the spirit of the open source community, ODRL is freely available. It was recently accepted by the Open Mobile Alliance (OMA)²⁵⁰ as the standard REL for mobile content. The latest version of the ODRL specification (Version 1.1) was co-published by W3C (as a W3C Note). The OpenIPMP Open Source Rights Management Project²⁵¹ have just released the first version of their DRM software that utilises ODRL as the Rights Expression Language.

²⁴⁸ See: Iannella (2002).

²⁴⁹ See: <http://www.odrl.net>.

²⁵⁰ See: <http://www.openmobilealliance.org>.

²⁵¹ See: <http://www.openipmp.com>.

IV.2 XrML

The eXtensible rights markup language²⁵² is an REL specification developed by ContentGuard, a joint venture set up by Xerox and Microsoft. Like ODRL, XrML has also been accepted by standards bodies. XrML Version 2.0 was selected as the basis for development of the MPEG 21 Part 5 standard for an REL (see page 106) and for the Open eBook Forum²⁵³ (OeBF) standard REL. The REL standard of the Organization for the Advancement of Structured Information Standards²⁵⁴ (OASIS) will be based on XrML Version 2.1. ContentGuard has discontinued further development of XrML and transferred this responsibility to the OASIS *Rights Committee* and the MPEG initiative. However, the rights for industrial use of XrML functionality still need to be licensed with ContentGuard.

IV.3 The <indec> 2rdd Project

The <indec > 2rdd project is based on the <indec > project, which defined a framework for interoperable metadata in content-based e-commerce and is now hosted by the DRM consulting company Rightscom²⁵⁵. In contrast to ODRL and XrML, the project focuses exclusively on defining a rights data dictionary, and its objective is to complete the MPEG 21 Part 6 standard for an RDD.

IV.4 MPEG 21

The Moving Pictures Expert Group (MPEG) is the ISO/IEC working group in charge of developing standards for the coded representation of digital audio and video. Among other standards, MPEG is working on Standard 21 with a view to developing a standardized multimedia framework. Parts 5²⁵⁶ and 6²⁵⁷ of Standard 21 specify an REL and RDD suitable for such a framework. After defining the *requirements for RELs and RDDs*²⁵⁸, MPEG issued a call for contributions to select one REL and one RDD as a basis for future development. XrML Version 2.0 was accepted as the future MPEG 21 rights language, and the data dictionary from the <indec > initiative was accepted as the basis for Part 6 of the MPEG 21 standard.

IV.5 Other Initiatives

XrML and ODRL are the leading initiatives in the field of rights expression languages. There have been other approaches which have been partly merged into one of the two languages or have not seen further development, while other

²⁵² See: ContentGuard (2000).

²⁵³ See: <http://www.openebook.org>.

²⁵⁴ See: <http://www.oasis-open.org>.

²⁵⁵ See: <http://www.rightscom.com>.

²⁵⁶ See: DeMartini, Wang, Wragg (2002).

²⁵⁷ See: MPEG-21 RDD (2002).

²⁵⁸ See: MPEG-21 Requirementants (2002).

newer initiatives are not yet established. This subsection briefly addresses these approaches and other appreciable initiatives as well as their status.

- RealNetworks, Inc. has put effort into its eXtensible Media Commerce Language (XMCL). An earlier version of XMCL was merged with ODRL in November 2001, but the language is still being developed independently.
- A relatively new initiative is the DREL (Digital Rights Expression Language) project founded in 2002 by the IEEE Learning Technology Standards Committee (LTSC)²⁵⁹. This committee addresses the need to express digital rights in the context of education.
- Xerox has done pioneering work in developing the Digital Property Rights Language (DPRL). DPRL was the precursor of XrML and is not being developed further.
- OASIS has just released Version 1.0 of the eXtensible Access Control Markup Language (XACML). XACML focuses on expressing access control policies rather than high-level usage rights for digital goods or services.
- The eBook industry has just started working on their “Rights Grammar” specification in order to develop a standard that provides interoperability among DRM systems in the eBook community.
- The Custom Digital Rights Language (CDRL)²⁶⁰ is being developed by Octalis. Octalis²⁶¹ is a spin-off of a Belgian University and of no importance in the current DRM industry or standards bodies.
- The Creative Commons initiative, founded in 2001, aims at defining licenses to support rightsholders to assign the public domain specific rights to their creative works²⁶². The initiative is developing a metadata format to express these licenses.

All of the major standards bodies as well as the publishing industry are aware of the need for a rights expression language and thus involved in some kind of REL development projects.

V Application Fields

The fields of application for rights expression languages are numerous and have not yet been exhausted. This section introduces a number of current and potential application fields for RELs, starting with an enumeration of typical use scenarios.

1. Rights expressions can be used in secure digital containers. A secure container is a transport format for digital goods.²⁶³ Its minimum components are the digital good in encrypted format and the corresponding rights information. The secure container grants access rights to authorized users only.

²⁵⁹ See: <http://ltsc.ieee.org>.

²⁶⁰ See: Octalis (2002).

²⁶¹ See: <http://www.octalis.com/>.

²⁶² See: Creative Commons (2002).

²⁶³ See: *Spenger* within this book on page 62.

The rights expressions are interpreted and processed by the appropriate secure viewer, i.e., the software designated to handle the secure container and render the content appropriately. For example, EMMS, which is IBM's DRM system (see page 111), uses this technique to package and distribute content (formerly *Cryptolope* technology). Microsoft's WMA format is another implementation of secure container technology.²⁶⁴

2. As an alternative to 1., access rights and digital goods/services can also be distributed separately. For example, the encrypted digital good or service can be distributed by means of superdistribution (e.g., peer-to-peer technology). Prior to accessing the product, the user has to receive the appropriate rights, which are sent separately in the form of a ticket (also called a voucher). Nokia is currently developing such technology²⁶⁵ for the mobile communications sector.
3. In general, rights expression languages have the power to express offers and contracts (or agreements). Digital offers and contracts become legally binding with the digital signatures of the contracting parties. Digital contracts are a driving technology and a critical success factor in electronic business, regardless of whether the subject matter of the contract is a tangible/intangible or digital/physical product.

Hybrids and alternatives of the variants above are also conceivable in the technical application of rights expressions, depending on the system architecture and the information flow designed in the DRM system (see page 154). Generally speaking, the main field of application for rights expressions formulated with an REL will be the exchange of rights information between interoperating systems, independent of the logical construct they represent (contract, offer, etc.).

In order to integrate an REL into an information system, at least two components have to be added²⁶⁶:

- *License phrasing component.* The license phrasing component supports the user in writing rights expressions. This component could be, for example, a web-based user interface that helps content providers create offers. An REL instance is generated by the license phrasing component according to the specifications of the content provider.
- *REL interpreter.* A detailed REL instance is useless without an XML interpreter which is able to read and process the REL. For example, a secure viewer in charge of handling a secure container must be able to interpret the rights expressions which accompany the content in order to grant access to and render the content accordingly.

The interpretation of a rights expression forms the basis for its enforcement. The enforcement of a rights expression refers to the execution of the rights granted

²⁶⁴ To learn more about secure containers see: *Spenger* within this book on page 62.

²⁶⁵ See: Nokia (2001).

²⁶⁶ See: Guth, Simon, Zdun (2003).

in accordance with the intentions of the rights holder. Further reading on rights enforcement can be found in Guth and Koeppen²⁶⁷.

RELs are often more powerful than the DRM system requires. Therefore, the rights expression language is usually adapted to the specific implementation and domain, and adaptation policies are developed to specify the restrictions or subset used. Examples of policies include defining the vocabulary used, naming the identification schemes allowed in instances (e.g., DOI, ISSN) or restricting the depth of nested rights expressions. The license phrasing component and the REL interpreter have to implement these policies.

The main focus of this section was to introduce ways to assign rights expressions to digital goods or services and to control usage and access. However, the machine-readable information in rights expressions or contracts has more potential than simply supporting access control. For example, electronic contracts can be used as an information base for customer relationship management services, contract-based workflow management, financial controlling or intellectual property rights discovery and protection.

VI Practical Examples

All current RELs are defined using XML technology²⁶⁸, which means that the language concept and the data dictionary are defined using XML schemas or data type definition (DTD) documents. Consequently, valid rights expressions are instances of the REL schemas or DTDs.

VI.1 ODRL Example

ODRL Version 1.1 comprises two XML schemas: one which defines the language concept and a second that defines the ODRL rights data dictionary. The following code is a simple example of ODRL showing a contract for a video (disregarding XML namespace labels). ODRL uses XML attributes to assign additional information to the vocabulary (cf. “currency” of the amount tag).

The sample license shows a recording of a marketing lecture sold to the *Université Libre de Bruxelles* for the price of €10 with the right to *play* the video *five times*. The video stream’s rights holder is the *Department of Information Systems at the Vienna University Economics and BA*. In this example, we used proprietary IDs from the Universal Project²⁶⁹.

²⁶⁷ See: Guth, Koeppen (2002).

²⁶⁸ See: Fallside (2001).

²⁶⁹ See: <http://www.ist-universal.org>.

```

<rights>
  <agreement>
    <party>
      <context>
        <uid>urn:univ:us-wuw-deptIS </uid>
        <name>Department of IS, Vienna University of Economics and BA</name>
      </context>
      <rightsholder/>
    </party>
    <asset>
      <context>
        <uid>urn:univ:lr-wuw-vid-1</uid>
        <name>Marketing strategies for Universal</name>
      </context>
    </asset>
    <party>
      <context>
        <uid>urn:univ:us-wuw-uniBrux</uid>
        <name>Université Libre de Bruxelles</name>
      </context>
    </party>
    <permission>
      <play>
        <requirement>
          <prepay>
            <amount currency=EUR>10.00</amount>
          </prepay>
        </requirement>
        <constraint>
          <count> 5 </count>
        </constraint>
      </play>
    </permission>
  </agreement>
</rights>

```

VI.2 XrML Example

The XrML Language is defined by three XML schemas: the XrML core schema, the XrML standard extension (sx) schema and the XrML content extension (cx) schema. This example includes XML namespace information, which is necessary for the validation of XML instances. XrML envisages the use of XML Signature specifications to describe the identity of the contracting parties. The example below shows an XrML instance which reuses elements of the XML Signature namespace.

The “license”-tag is the root element of an XrML instances, asset and party are referred to as the “resource” and “principal” in the basic language concept of XrML. “Grant” comprises the actual rights expression. Rights are expressed as

“rights” plus “conditions”. The XrML-compliant representations of the resource and principal are “digital work” and “keyHolder.” The XrML vocabulary contains “print” and “validityInterval” as a right and condition. The XrML license below grants the owner of the x509 certificate the use of *someResource.xxx* until the *end of year 2005*.

```
<?xml version="1.0" encoding="UTF-8"?>
<license xmlns="http://www.xrml.org/schema/2001/11/xrml2core"
        xmlns:sx="http://www.xrml.org/schema/2001/11/xrml2sx"
        xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:cx="http://www.xrml.org/schema/2001/11/xrml2cx"
        xsi:schemaLocation="http://www.xrml.org/schema/2001/11/xrml2cx
        ..\schemas\xrml2cx.xsd">

  <grant>
    <keyHolder>
      <info>
        <dsig:x509Data>
          <dsig:X509IssuerSerial>
            <dsig:X509IssuerName>CN=Guth Susanne,
              OU=Dept. of Information Systems,
              O=Vienna University of BA, L=Vienna,
              ST=Vienna, C=Austria
            </dsig:X509IssuerName>
            <dsig:X509SerialNumber>12345678</dsig:X509SerialNumber>
          </dsig:X509IssuerSerial>
          <dsig:X509Certificate>MIIEDCCA6GgAwIBAgIBEDANBgkqhki...
            ...Zos6NAm8m6UQBA== </dsig:X509Certificate>
        </dsig:x509Data>
      </info>
    </keyHolder>
    <cx:print/>
    <cx:digitalWork>
      <cx:locator>
        <nonSecureIndirect URI="http://www.wu-wien.ac.at/someResource"/>
      </cx:locator>
    </cx:digitalWork>
    <validityInterval>
      <notAfter>2005-12-24T23:59:59</notAfter>
    </validityInterval>
  </grant>
</license>
```

VII Current Market Situation and Trends

This section examines the application of rights expression languages in the current DRM systems market. The leading developers of DRM middleware include IBM, Adobe, Real Networks and Microsoft, although Real Networks is currently not using an REL in their products.

- IBM has developed a product called the Electronic Media Management System (EMMS)²⁷⁰, which currently deploys a proprietary rights expression language influenced by ODRL. EMMS supports a variety of media formats. IBM is working in close cooperation with Nokia to develop solutions for the mobile communications sector²⁷¹. Nokia has just released a new version of their content publishing toolkit, that provides for content creation in the OMA format (based on ODRL) and enables deployment of content and rights to mobile handsets.
- Microsoft has implemented XrML in its Windows MediaTM Rights Manager. This software provides a means of packaging content and specifying usage and access rights formulated in XrML. The output of this tool is a file in Windows Media format (WMA), and the rights can be interpreted and processed by the Windows Media Player.
- Adobe offers DRM solutions for the exchange of documents in pdf format, including e-Books. The documents are created with the Adobe Content Server software and can be interpreted and enforced with the corresponding reader, which offers the functionality of a secure viewer. Adobe is a supporter of the ODRL initiative and a DRM player which will potentially use ODRL in future products.

Based on this middleware, some implementations have already appeared on the Internet. One of the first music subscription services, PressPlay²⁷², uses the Microsoft solution and thus works with XrML. MusicNet²⁷³ is a digital music service based on Real Networks' technology. The M-Stage Mobile Music Service²⁷⁴ is a product on the Japanese mobile-commerce market hosted by NTT DoCoMo, based on IBM's EMMS technology. Besides the market leaders, there are also other projects which have implemented rights languages, such as the COLIS²⁷⁵ project, which uses ODRL.

InterTrust, one of the pioneers in the development of specifications for DRM systems, does not provide a DRM middleware implementation. However, InterTrust has recently had success in licensing its DRM specifications.

All REL developers publish up-to-date information on implementations of their languages as well as their supporters on their web sites. One reliable online source of information on RELs is OASIS' *The XML Coverpages*²⁷⁶

²⁷⁰ See: <http://www.ibm.com/software/data/emms/>.

²⁷¹ See: Nokia (2001).

²⁷² See: <http://www.pressplay.com/>.

²⁷³ See: <http://www.musicnet.com/>.

²⁷⁴ See: http://www.nttdocomo.co.jp/p_s/mstage/music/.

²⁷⁵ See: <http://www.colis.mq.edu.au/>.

²⁷⁶ See: <http://xml.coverpages.com/drm.html>.

2.3.6 Electronic Payment Systems

*Ahmad-Reza Sadeghi*²⁷⁷, *Markus Schneider*²⁷⁸

Abstract: With the development of digital rights management systems, new commercial applications for the trade with digital goods will be introduced, and new information services will be provided. As digital goods or services can be delivered over networks, it is also desired that they can immediately be paid electronically. Thus, it is assumed that the trade with digital goods stimulates the deployment of electronic payment systems. Furthermore, new commercial models make new demands on specialized payment systems, e.g., low-value payments should be supported in an economically reasonable way. Meanwhile, there exists a large body of literature on electronic payment system. In this paper, we give a survey of these systems. We point out the requirements they should fulfill and present briefly the basic principles for different categories of payment systems, and consider a few candidates.

I Introduction

Since the overcoming of barter in the history of mankind, trade usually involves the exchange of goods and equivalent abstract values, such as money. Over years, many variants have been introduced of how to pay and thereby handing over monetary values in commercial relationships, e.g., cash as coins, cash as banknotes, cheques, or early paper-based credit card payments²⁷⁹. This was before electronic payment systems.

With the dispersal of digitalization and the availability of communication networks, a large number of electronic payment systems have been proposed and developed which provide new means for the representation of values. Loosely spoken, in electronic payment systems monetary values are transferred electronically between a payer and a receiver. Note that exchange of values among financial institutions for the purpose of clearing is also carried-out electronically. However, clearing systems are outside our considerations here.

There were many reasons — technical and economical ones — driving the tremendous effort done in the area of electronic payment systems. Here, we restrict our considerations exclusively to technical aspects. Among them, two important reasons are:

- Security aspects: Traditional means for payment show various security problems such as counterfeit banknotes. One of the main goals of electronic payment systems was to achieve a higher level of security as offered by traditional systems, even if electronic payment systems introduce new kinds of threats.
- Commerce over communication networks: In case of commercial relationships where involved parties are connected over communication networks, traditional means for payment cannot be used anymore which assume physical

²⁷⁷ Saarland University, Computer Science.

²⁷⁸ Fraunhofer Gesellschaft, Institute for Secure Telecooperation.

²⁷⁹ See: Davies (1996).

contact. Thus, electronic business processes of geographically distant parties require that monetary values can be transferred over networks.

In the early years of doing business electronically up to now, most popular electronic shops were focusing predominantly on the exchange of physical goods, such as books or CDs. As experience has shown in this context, buyers have mainly used conventional payment systems either electronic or traditional, e.g., credit cards or bank transfer after delivery of goods. User behaviour varies in international context. Unfortunately, often more modern electronic payment systems that have been developed and tested in several field trials in the last years were not successful, and thus were not used in real life applications. There are many reasons having caused this²⁸⁰. For customers there was often no obvious reason to get used to new and complicated payment systems when they were able to manage the needs with their conventional payment systems. Furthermore, customers did not use specific payment systems which were not provided by a large merchant base. On the other hand, the low number of customers did not stimulate merchants to provide new electronic payment systems.

The growing market for digital goods supported by the availability of digital rights management systems may change some conditions regarding electronic payment systems. Digital goods allow that all phases of a typical business process from *search* to *delivery* are carried out electronically. Thus, it is reasonable for those business processes to also involve the electronic exchange of monetary values. This can be done immediately before or after delivery. In this context, electronic payment systems have to be usable for transferring value over networks such as the Internet. Furthermore, especially in the trade with digital goods, one may expect certain commercial relationships that require payments of low values, e.g., in the range from a few Cents to a few Euros. As an example for such a case consider a merchant that sells small-sized digital products like newspaper articles. In another example, a commercial model might be based on metered usage of digital products in a digital rights management system where a consumer has to pay low values for specific activities. Note that in general, electronic payment systems do not guarantee the delivery of purchased goods. Solutions for *fair exchange* are not the subject of this paper.

In the following, we will give an overview of electronic payment systems. Our aim is not to cover all electronic payment systems that have been proposed in the last 20 years. Instead, our intent is to summarize the most important requirements for electronic payment systems and to categorize them. Furthermore, we explain the basic concepts and principles which are applied in these categories in a rather abstract way, i.e., without going into the details of specific electronic payment systems. Nevertheless, we will mention some concrete proposals for each category. Finally, we will shortly present some current sample systems which are used in practice.²⁸¹

²⁸⁰ See: Yung (2000).

²⁸¹ Other work providing either short surveys or more comprehensive treatments of electronic payment systems can be found in: Asokan, Janson, Steiner, Waidner

II Models

In a commercial context, payment always involves a *payer* P spending money and a *merchant* M who receives the money. P and M may have accounts at distinct banks, B_P and B_M , respectively.

As for traditional payment systems, electronic payments can be carried out in many ways. Here, we consider the basic types of payment systems: cash-like, cheque or credit card, remittance, and debit order. The way how the exchange of real money among the banks is initiated in these systems varies as can be seen in Figure 1:

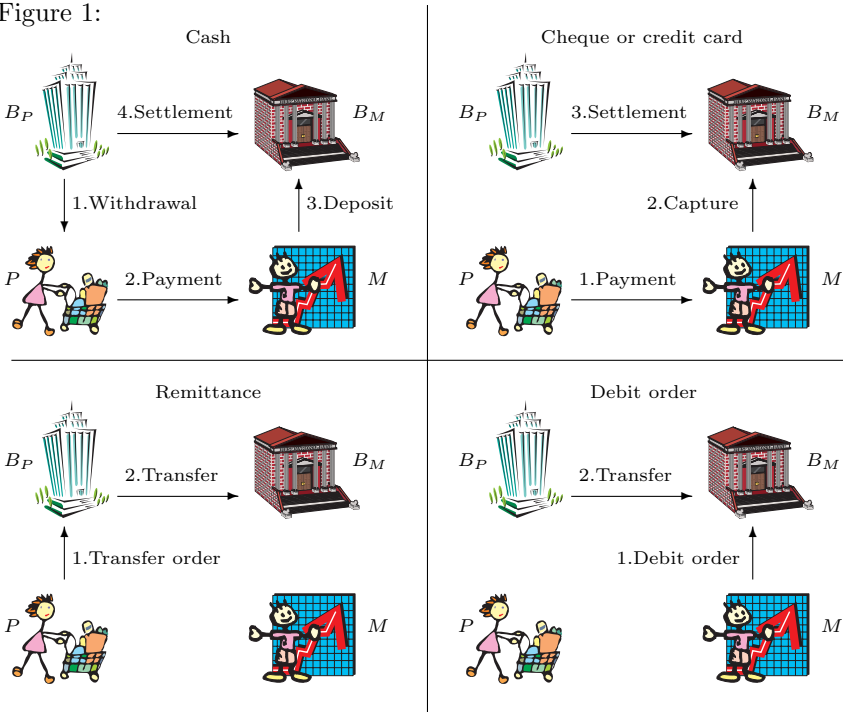


Fig. 1. Types of Payment Systems

In *cash* systems, P obtains electronic cash in the *withdrawal* phase from B_P . For this cash, B_P debits a corresponding amount of money from P 's account. Then P can start his purchases where she pays with this cash. In the *payment* phase, the cash is transferred to M . In the *deposit* phase M forwards the cash to his bank B_M that initiates the *settlement* phase in which real money is exchanged from B_P to M 's account at B_M .

Regarding the sequence of phases, *cheque* and *credit card* payment belong to the same category of payment systems. Both start with the *payment* phase in which

(1996/1997/2000); O'Mahony, Peirce, Tewari (1997); Pilioura (1998); Pfizmann, Waidner (1996); Schmidt, Schunter, Weber (1998); Jakobsson, MRaihi, Tsiounis, Yung (1999); Abrazhevich (2001a).

P sends a filled-in electronic form to M . In the *capture* phase, M hands this to B_M who receives the money from B_P in the *settlement* phase.

Both types above are *direct* payments since there is a direct interaction between the payer and the merchant. Another category of systems deals with *indirect* payments. In these, only one party, either P or M , is involved in the payment. *Remittance* and *debit order* systems belong to the category of *indirect* payments. Although, they are often used in electronic business relationships, we will not consider them here in detail. These systems are mainly based on financial networks and usually do not involve open networks such as the Internet. Here, our interest is more in modern payment systems that can be used over open networks.

Debit order systems may be suited for subscription models at large merchants. In such systems, the merchant periodically requests the payer's bank for the payment, e.g., monthly or yearly. But subscription models will only be deployed in such business models in which customers rather regularly request services or products, e.g., newspaper articles.

These basic payment models are surely helpful when classifying proposed electronic payment systems. However, there are also payment systems whose underlying model cannot be fully assigned to one of these basic models we have considered here.

In general, the choice of a payment system best suited for a specific commercial relationship may depend on various conditions, e.g., concrete systems supported by the merchant, trust in payment systems or organizations behind them, privacy requirements, additional costs.²⁸²

III Requirements for Payment Systems

In this section, we consider the main security and privacy requirements for electronic payment systems in general. Note that not all of these requirements are necessarily relevant and have to be fulfilled for all different types of payment systems which will be presented later. Requirements for systems usually vary according to their specific features and the underlying trust assumptions. In fact, there are also other important requirements for electronic payment systems, e.g., usability, acceptability, scalability, interoperability, availability²⁸³. However, due to space limitations, these will not be considered here.

III.1 Fraud Prevention

Similar to traditional payment systems, security aspects are of central interest for electronic payment systems. Thus, the prevention of fraud and theft resulting in monetary loss for honest parties and profit for malicious parties is an important requirement. Obviously, electronic payment systems have to cope at least with

²⁸² For more details see: Abrazhevich (2001b/c).

²⁸³ See: Abrazhevich (2001b/c); Schmidt, Schunter, Weber (1998).

the same threats as physical payment systems do; there is potential of minting and printing counterfeit money, forging cheques, stealing credit card numbers, and many more things adversaries might try. Electronic payment systems should require that the — usually contradicting — interests of all involved parties are protected.

One of the main security requirements is *unforgeability* of monetary value. This concerns various aspects:

- creation of new monetary value,
- modification of monetary value,
- overspending.

The first aspect deals with *data origin authentication* of digital monetary values. Since malicious parties cannot be prevented from attempting to forge, this guarantees that maliciously created monetary values can be detected. Another aspect considers the *integrity* of data which represent monetary values. It is necessary that amount modifications can be detected, e.g., changing the amount of an electronic cheque or electronic cash a posteriori. The next aspect of unforgeability stems from the fact that digital monetary values can be copied very easily where the original and copies are indistinguishable. Thus, electronic payment systems require *protection against overspending*. There are different strategies to do this: *overspending detection* where overspent copies are immediately detected at the moment of spending it, or *overspender tracing* where the overspending party can be identified afterwards.

Parties are also interested that no payments are actually initiated without their consent. This is tackled by the requirement of *authorization*. This involves aspects as to allow access to installations exclusively to their owners, and for parties / systems to act according to other parties' instructions only if these are authentic, or even better, if they are non-repudiable.

III.2 Confidentiality

Electronic payment systems should offer at least as much confidentiality as traditional payment systems currently do. The goal of this requirement is that payment data should not be exploitable in order to obtain more precise or more comprehensive information about involved entities, e.g., payer profiles. Thus, confidentiality properties of electronic payment systems can be distinguished regarding which information they reveal to which parties. Confidentiality of payment information against other parties can be achieved by encrypting communication which is no specific property of payment systems. Note that confidentiality in electronic payment systems cannot prevent information flows which may happen outside an electronic payment system among involved parties, e.g., by observing communication networks, or revealing data in further commercial interactions.

Preventing undesired linking of specific information to identities can be achieved by anonymization techniques. Electronic payment systems can have different goals regarding the realization of anonymity, i.e., who should be anonymous

from whom. Note that confidentiality is not necessarily achieved by only using anonymization techniques. Obviously, anonymity is only possible if the set of people which are potential candidates is large enough. Technically, one can also distinguish among different types of anonymity. In a system in which a party does not obtain another party's identity, it may still be possible to link several activities (e.g., payments) stemming from the same party. In systems providing *unlinkability* no relations among different actions in the electronic payment system can be established, e.g., to link payments of the same payer.

Most proposals focus on privacy concerns of payers when banks get insight at which merchants they buy²⁸⁴. From such information, banks may come to further conclusions which the payer might want to prevent; e.g., when a bank gets aware that a payer often buys at pharmacies it may draw conclusions about the general health of the payer. In this context, electronic payment systems with payer anonymity against the bank are of interest. This means that monetary values obtained by the merchant from the payer and then forwarded to the bank should not reveal the payer's identity. There are also some proposals dealing with recipient anonymity²⁸⁵.

In an electronic payment system in which a party is completely anonymous against other parties, there is the risk that anonymity may be misused, e.g., in case of money laundering or blackmailing²⁸⁶. Thus, there are proposals in which anonymity can be revoked under certain circumstances, such as *escrowed payment systems*.

III.3 Fault Tolerance

There is a requirement to protect parties from financial losses in case of system crashes and network failures. Parties have a strong interest to be safeguarded against financial loss because of events which are beyond their control. Thus, electronic payment systems require that parties can be reimbursed for monetary value they have lost. Obviously, these solutions have to take into consideration parties that falsely claim a loss and maliciously try to achieve a profit.

Furthermore, electronic payment systems have to follow the transaction concept in order to guarantee that they always are in a consistent state. This means that a payment protocol is atomic, i.e., it is either executed completely or not at all.

IV Properties of Payment Systems

In this section, we present some of the main properties of electronic payment systems that should be considered when comparing systems or selecting a system for a special purpose or application.

²⁸⁴ See: Chaum (1983/1986); Chaum, Fiat, Naor (1990).

²⁸⁵ See: Chaum (1989).

²⁸⁶ See: Sander, Ta-Shma (1999); Solms, Naccache (1992).

IV.1 Small- and Low-Value Payments

Small- and low-value payments require low transaction costs. If a product's price, e.g., for a web page, a single music file or a newspaper article, is in the range of only some Cents or even smaller, then the overhead costs for a credit card payment would be a multiple of the costs for a product (e.g., for sample costs see Jakobsson, MRaihi, Tsiounis, Yung/ Micali, Rivest²⁸⁷). Sometimes, even many small amounts have to be paid to the same merchant for different products where it is not possible to pay the sum of all these amounts at once, e.g., for telephone calls. Thus, efficient and low-cost processing of low-value payments requires specific electronic payment systems. Such micropayment systems are assumed to be of considerable importance for commerce focusing on digital goods. Since high processing costs of some systems also stem — among other reasons — from their high computational effort (e.g., because of digital signature generation), application of efficient primitives is necessary. As a consequence, the security level of micropayment systems may be lower. This may be justified because lower values imply smaller risks. Beside computational costs, efficiency in micropayment systems has further aspects. In more efficient micropayment systems, merchants can request the monetary value from the payer's bank for aggregated micropayments received from one payer by simply presenting one single payment item instead of forwarding every micropayment item. Obviously, such a solution does still not help if a payer spends only some Cents. For such cases, other solutions for cost aggregation are required.

IV.2 Divisibility

For real cash, a payer is either required to have the right denomination, or change will be given to her. In the context of anonymous electronic cash systems, change may be undesired. In contrast to real world cash, divisibility of electronic cash is possible²⁸⁸, i.e., electronic cash can be splitted into smaller values in order to achieve the desired denomination. Thus, a user of a divisible cash system is always able to pay the required amount provided she has enough money. This property can be easily achieved with cheque or credit card payment.

IV.3 Transferability

Traditional cash can be flexibly exchanged among users without the necessity of involving the money issuer. For reasons of cost reduction, flexibility, and usability, users will prefer electronic payment systems that allow transferability of monetary values just as traditional systems do. In electronic payment system literature, transferability is mainly considered for digital cash systems. In most proposed electronic cash systems, cash is only for payments by those parties that have withdrawn them, i.e., transferability is not supported.

²⁸⁷ See: Jakobsson, MRaihi, Tsiounis, Yung (1999); Micali, Rivest (2000).

²⁸⁸ See: Chan, Frankel, Tsiounis (1998); Okamoto, Ohta (1992).

IV.4 Offline Usability

Payment systems should be universally usable, i.e., they should be usable under many circumstances and conditions. This prevents users from being required to deal with multiple payment systems in parallel which may bring some confusion in overviewing their financial status. Thus, even if electronic payment systems are mainly developed to be used for the exchange of monetary values over the Internet, they should also be usable if a payer is not online on the Internet.

IV.5 Financial Status Transparency

In order to plan purchases and economical decisions users appreciate a possibility to have an overview of their financial status. This is easily possible with traditional payment systems by just having a look in the purse or the bank account. Thus, users of electronic payment systems may require a similar property. The possibility for checking the current balance should be given anytime and anywhere. Obviously, it is advantageous if users are able to check their financial status before proceeding to a cash desk. Furthermore, users usually prefer to check their balance privately.

IV.6 Cost Efficiency

Every payment system — both traditional and electronic — produces some overhead costs. Obviously, costs are very important for user acceptance. These costs are caused by many influences which we cannot list here completely. For electronic payment systems these costs may stem from costs for communication networks, for infrastructure and other investments required at banks, merchants and for the payer, e.g., a specific payment device or an electronic wallet, and also fees banks charge for the processing of payments.

V Classification

In general, there are many ways to classify electronic payment systems. In the following, we will consider some aspects according to which one may classify electronic payment systems.

V.1 Online or Offline

Online payment systems involve a third party, e.g., a financial institution, for each payment. This institution usually verifies whether a payment can be accepted, and if yes, then it authorizes the payment. For instance, online verification of digital payments is used for overspending detection, or the payer's solvency. In contrast, offline systems do not require connecting to such a third party, and therefore, they require less communication. Thus, offline systems lower the costs for payments. In an offline system, a merchant can collect payments received over some period of time, e.g., a day, and then forward the collected pay-

ments at once. In general, payments involving larger amounts of money should rather be done by using online systems whereas for lower amounts one could use offline systems.

V.2 Pre-paid, Pay-Now, or Pay-Later

Another aspect of a payment system is the time when the payer's account is debited. In *pre-paid* systems, the account is debited before purchase. This happens in a *withdrawal* phase. Usually, payers do not prefer the pre-paid variant. Pre-paid systems have the disadvantage for payers that they lose potential interests since they have to withdraw money from their account before the payment occurs. In *pay-now* systems, the payer's account is debited at the time of payment. In *pay-later* systems, the merchant's account is already credited at the time of payment, but the payer's account is debited later.

V.3 Hardware-Based or Software-Based

Payment systems can be based on hardware, software, or some kind of hybrid solutions. Hardware-based and software-based systems differ in the way how security is achieved. Hardware-based approaches achieve security by the usage of tamper-resistant hardware^{289,290} The idea of such a hardware is that users cannot manipulate the amount of money they own. Examples for such hardware are smartcards or PDA-like electronic wallets. In principle, software-based systems allow the manipulation of data, but they should prevent that malicious parties obtain any profit out of such manipulations. Thus, software-based systems are usually designed as online payments where a third party verifies the payment whether it is acceptable. There are also hybrid solutions which combine protection means of hardware and software²⁹¹.

V.4 Anonymous or Non-anonymous

The majority of existing systems does not fulfill the confidentiality and privacy requirements we have considered above. If electronic payment systems do not anonymize customers to a sufficient degree, banks are able to collect great amounts of data about their customers. For data mining reasons, this collected information has a considerable value for banks. It can be exploited for own reasons, e.g., discrimination and marketing, or it can be sold to other parties. Anonymous systems prevent this kind of threats. Of course, electronic payment systems cannot prevent information leaks that occur outside the payment system. If payers are interested to protect their personal information then they should decide for an electronic payment system that provides anonymity. Unfortunately, anonymity is usually sacrificed for cost reduction and potential misuse.

²⁸⁹ Note that tamper-resistancy is a strong assumption. Using sophisticated equipment one can attack hardware components

²⁹⁰ See: Anderson, Kuhn (1996).

²⁹¹ See: Brands (1993b).

For the future, there is a need for privacy protecting micropayment systems in order not to lose the important goal of personal data protection.

V.5 In-Band or Out-Band Authorization

Before the bank credits a merchant's account it usually verifies whether the payment is really authorized by the payer. There are several possibilities for the payer to give this authorization to the bank. Thus, some payment systems have a technical method for the provision of such an authorization, e.g., by sending a password or a digital signature to the bank in order to verify that the payer agrees to the payment. Digital signature can provide non-repudiation of the authorization. When the payer's authorization is directly given within the payment system, we call this *in-band* authorization. In other cases, there is no method provided by the electronic payment system itself. Then, we talk of *out-band* authorization. In such systems, the payer can send his authorization on another channel, e.g., authorization via phone, or absence of complaints over a certain period of time is interpreted as authorization. For instance, out-band authorization is used when in-band authorizations over the Internet are assumed to be insecure. On the other hand, out-band authorization may make the payment awkward.

V.6 Cryptography-Based or Cryptoless

Electronic payment systems may apply cryptography or not. Systems which do not use cryptography should not be used for payments over the Internet. Cryptoless systems should involve out-band activities in the payment process. If one can assume a sufficiently high level of security for an authenticated origin then the risk is not too high. However, if the goal is to carry out the whole payment process over the Internet, then one should definitely choose a payment system that applies well-selected cryptographic primitives and protocols.

V.7 Probabilistic or Deterministic

The majority of electronic payment systems employs deterministic methods in all system phases (e.g., withdrawal, payment, deposit). However, there are proposals for electronic payment systems that involve probabilistic methods. The motivation behind this was to reduce costs by increasing the efficiency throughout multiple payments. The application of these techniques was proposed for micropayment systems. In proposed approaches, one can distinguish among the ways according to which probabilistic decisions are applied. These are probabilistic *payment* and probabilistic *verification*. Probabilistic *payment* means that for each payment, the payer and the merchant interact according to a pre-determined process so that with a certain probability a payment is selected, otherwise discarded. In probabilistic *verification* approaches, the merchant initiates a payment verification according to a probabilistic function.

VI Electronic Cheques

A cheque is a payment order addressed to a certain payee and signed by the payer to transfer a certain monetary value from the payer's account to the payee's account. Usually, the payee also signs the cheque and gives it to her bank which takes care of clearing with the bank of the payer. Electronic cheques were assumed to replace the conventional paper-based checks to reduce the processing, transport and communication costs. Basically, an online verification must be done in a purchase to ensure that the underlying cheque is backed. However, to reduce the communication overhead an offline verification would be sufficient. In the following, we present some proposals for electronic cheque systems.

An electronic cheque architecture was designed and implemented by the *Financial Services Technology Consortium* (FTSC)²⁹². This system requires that authorized users obtain a smart-card based electronic chequebook device which is assumed to be tamper-resistant. This device stores information such as signing key and certificates and has the role of an observer taking care of the cheques that have been issued previously. The payee should possess a similar device. After the payee forwards the cheque to his bank, the financial network takes care of authorization and clearing.

Another electronic cheque system is contained in the *NetBill* system²⁹³. It intends to provide a complete trading system from the *negotiation* phase to the *delivery* of goods. In the negotiation phase, the buyer and the merchant agree upon terms and conditions. For the buyer to be able to obtain the good, the merchant must verify the validity of the cheque where a third party, the *NetBill* server, is involved in the payment. *NetBill* payments require mutual identification of the involved parties. This procedure is based on a modified version of *Kerberos*²⁹⁴, i.e., to use public key cryptography on the top of symmetric cryptography.²⁹⁵ Another online cheque-like system also based on *Kerberos* is *NetCheque*²⁹⁶.

One of the properties of common cheque systems is their auditability, i.e., they allow banks to identify payers and payees. Unfortunately, this property is in contradiction with the requirement concerning privacy protection, since it allows a bank to monitor the spending patterns of the payer.

VII Credit Card Payments

Payment systems based on credit cards are widely established payment methods, and have been in use for many years. In reality, one can distinguish between credit card associations and banks. However, for the sake of simplicity, we call them banks. In a purchase, the merchant asks the payer for card information (e.g., number, expiry date), and depending on his policy, the payment may be

²⁹² See: Anderson (1998).

²⁹³ See: Sirbu, Tygar (1995).

²⁹⁴ See: Steiner, Neuman, Schiller (1988).

completed at this point, or the merchant makes an online verification with the bank regarding the payer's solvency.

To be able to transport purchase and credit card information in a secure and authentic way over the Internet, the payer and the merchant can apply cryptographic protocols such as *Secure Socket Layer (SSL)*²⁹⁵. The IETF has adopted the *SSL* protocol and renamed it to *Transport Layer Security (TLS)*. This protocol is widely used for credit card payments in practice, however, it is no payment system. This protocol is rather a standard that provides secure channels and data authentication for *http* communication. The driving idea for the development of the *SSL* protocol was to secure the transmission of credit card numbers. This protocol allows an authentication of the merchant server (payer authentication is optional) after which a secure communication channel is established between the payer and the merchant, i.e., all messages are encrypted. However, protocols like *TLS* cannot take care of other issues required for electronic commerce transactions, e.g., for verifying the validity of the credit card, authorizing the payment, and interaction with clearing processes. Another problem is that the merchant is not prevented from accessing and misusing purchase information (e.g., card information). Moreover, it does not provide non-repudiation against cheating parties. Note that this requirement is crucial for promoting trade over the Internet. Nevertheless, *SSL/TLS* is widely used today for credit card payments over the Internet.

In parallel to this, more specific credit card systems for Internet payments have been developed which were not successful at the market. For instance, there have been *First Virtual* and *CyberCash*. *First Virtual* was shut down in 1998. It satisfied a minimum level of security by password authorization for payments, but did not apply cryptographic techniques. *CyberCash* credit card payment²⁹⁶ was contained in a comprehensive concept integrating distinct types of Internet payments. It applied public key cryptography which provided higher level protection for purchase data and authorization reasons.

Another development to be mentioned here is *i-Key Protocol (iKP)*²⁹⁷. Historically, it is an important system for further developments in this area, even if it is not used in real world applications. The models of *iKP* involve a third party acting as a payment gateway between the users of the system and the existing financial network. The main role of this gateway is to authorize the payment. During a purchase, the merchant sends the purchase data (e.g., credit card number, etc.), he obtained from the payer, to the gateway which forwards this information to the bank network where it is decided whether to authorize the payment. The result is sent back to the merchant through the gateway. The

²⁹⁵ *Kerberos* is a trusted third party authentication service enabling servers in an open distributed environment to control access and to authenticate requests for services.

²⁹⁴ See: Neuman, Medvinsky (1995).

²⁹⁵ See: Dierks, Allen (1999); Freier, Karlton, Kocher (1996).

²⁹⁶ See: Eastlake, Boesch, Crocker, Yesil (1996).

²⁹⁷ See: Bellare, et al. (1995); Bellare, et al. (2000).

payment system iKP ($i = 1, 2, 3$) represents a family of payment systems where i indicates the number of parties who possess an own key pair. For instance, in $3KP$ all involved parties, i.e., the payer, the merchant and the gateway have private / secret key pairs whereas in $2KP$ the buyer is the only one without own key pair. Individual protocols differ in both complexity and degree of security. To deal with non-repudiation, each of the involved parties (payer, merchant and gateway) can generate digital signatures. To protect payer's sensitive information from the merchant, all messages from the payer to the gateway via the merchant are encrypted with the gateway's public key.

iKP is a precursor of the well-known *Secure Electronic Transaction (SET)* standard²⁹⁸. The *SET* protocol was jointly developed by a consortium of credit card associations, among others. It enhances the earlier protocols by improving the cryptographic protection mechanisms for purchase details and allowing to use a certification authority hierarchy.²⁹⁹ From the today's perspective, it can be stated that the high expectations concerning the deployment of *SET* have not been fulfilled. Now, some remarks are in place.

- As mentioned before, iKP and *SET* use digital signatures to authenticate messages and authorize transactions where these digital signatures should make the parties' authorizations non-repudiable, i.e., provable to a third party. However, one has to take care of which kind of statements which participants in a payment may want to prove and can prove, and what are the requirements for provability in payment protocols³⁰⁰.
- Payment protocols with features as offered by *SET* are computationally costly since they require to carry out quite a number of expensive computations such as of digital signatures. Moreover, such systems operate *online* involving a third party payment gateway for the purpose of authorization and clearing. However, this leads to additional communication overhead. Note that the offline version would reduce this, however, it cannot prevent the misuse of card information.
- The mentioned credit card schemes do not protect the privacy of the payer since banks can identify the payer and monitor payer's commercial relationships, e.g., on card information or her signature verification key. In order to protect the payer's privacy against collecting behavioristic profiles, some solutions have been proposed to make credit card transactions anonymous³⁰¹. However, the anonymity can be revoked if several parties collude and compare the transcripts of payment processes. To our knowledge, these proposals are not applied in real world solutions.
- Today, credit cards are often used for Internet payments. They also have some advantages to be used in international commercial relationships where other systems like cheques, remittance, or debit order payments are rather

²⁹⁸ See: SET (1997a/b/c).

²⁹⁹ A certification authority is an infrastructure component that certifies public keys of the involved parties such as cardholders, merchants, banks.

³⁰⁰ See: Herreweghen (1996/2000).

³⁰¹ See: Low, Maxemchuk, Paul (1994).

unsuitable, e.g., due to high overhead costs. The costs for one credit card payment are currently in the range of about 20 – 40 Cents, with a little extra charge if they are used in a international context. Thus, they cannot be used for low-value payments.

VIII Cash Systems

Electronic cash is broadly defined as electronically stored monetary value³⁰². It intends to realize real world cash in an electronic way exploiting the merits of digital technologies. Nevertheless, electronic cash is often debated as a replacement for conventional cash, in particular, because it is expected to be less costly. Internationally, there have been many trials to introduce electronic cash products into the market, e.g. see CPSS BIS³⁰³. For electronic cash to really replace traditional cash, however, it should provide typical properties such as offline usability, privacy (pseudonymity, unlinkability), transferability and unforgeability (see Sections III and IV and also Schmidt, Schunter, Weber³⁰⁴, or CPSS BIS³⁰⁵). Unfortunately, until now there is no electronic cash system capable of satisfying all these requirements.

Over the past years a large number of electronic cash systems have been proposed offering different security levels and properties. In particular, designing *anonymous cash systems* has attracted many researchers. Most of these proposals offer only *payer anonymity* and only in the *payment phase*, but with *unlinkability*, i.e., the merchant, bank or their collusion cannot link a payment to the corresponding withdrawal.

The best-known systems in this class apply a cryptographic primitive called *blind signatures* to implement anonymity. These systems are also called *coin systems* on which we will mainly focus in the following.

The ingenious concept of *blind signatures* was introduced by Chaum³⁰⁶. Other than a normal signature, a blind signature is issued by an interactive protocol between a signer and a receiver. At completion of this interaction, the receiver obtains a signature on the message to be signed while the signer knows neither the message nor the signature on it. Loosely speaking, the goal is to prevent the signer from relating a signature, it observes later, to the receiver. This is called *blindness* requirement.³⁰⁷ At first glance, the idea of blind signatures sounds odd, however, it can be employed for constructing privacy protecting cryptographic

³⁰² See: CPSS BIS (1996).

³⁰³ See: CPSS BIS (2000).

³⁰⁴ See: Schmidt, Schunter, Weber (1998).

³⁰⁵ See: CPSS BIS (1996).

³⁰⁶ See: Chaum (1983/1984/1985).

³⁰⁷ More precisely, blindness means that given a set of transcripts of the blind signature protocol-runs, and the set of message-signature pairs generated by these protocol-runs, the signer cannot associate the protocol-runs with the message-signature pairs with a probability significantly better than pure guessing.

applications such as anonymous electronic cash. The basic idea is illustrated in Figure 2 and described in the following.

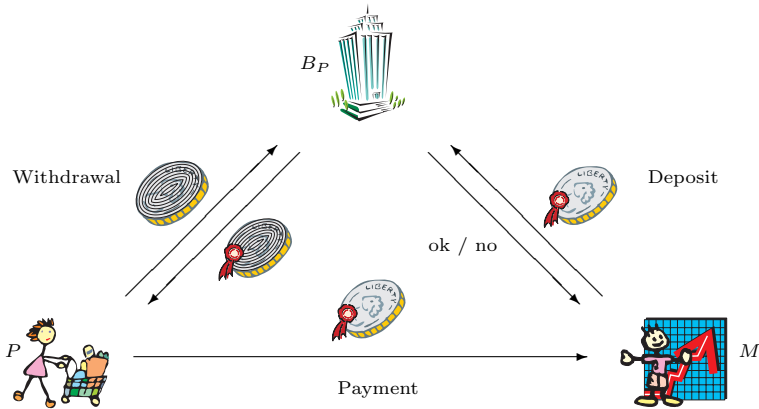


Fig. 2. Blinding of Digital Coins

During withdrawal, the payer P generates a coin c . The bank as the issuer of electronic coins signs these using a blind signature. This means, P blinds c by applying an appropriate transformation. We denote the blinded coin with c' , which is depicted by the shaded coin in Figure 2. P sends the blinded coin c' to the bank B together with a withdrawal order. This order contains mainly information about P 's account and the amount of money she wants to withdraw for this coin, e.g., 1 Euro. The bank B debits P 's account by the corresponding amount and signs c' with a signing key of a special public key pair which indicates c 's value. We denote the resulting signature with σ' .

During payment, P unblinds the signature σ' to a signature σ which corresponds to the unblinded coin c . P sends the pair (c, σ) to M who verifies the signature with the verification key of the bank.

During deposit, B verifies the validity of the coin by verifying σ , and verifies against double spending, i.e., it searches in its database whether this coin has been deposited before. If both verifications are true, B accepts the coin, deposits the corresponding value to M 's account, and sends the result to M . If M agrees, he may sign a receipt for P .

Note that we restrict our considerations to the basic principles common to most cash systems. However, for secure and real life application, one requires further measures.³⁰⁸

An important security requirement on cash systems is *double spender identification*. This is a mechanism which allows the bank to link double spent cash to the

³⁰⁸ For instance measures to provide secure dispute handling between the involved parties. Disputes may arise when a party claims that its statement of account is not correct, or the bank considers a coin as double spent, but, the payer claims the opposite (see Pfützmann, Waidner, Pfützmann (1987/2000) for a comprehensive discussion).

withdrawal of a payer and consequently identify this payer. This problem is less important in case of online systems since the bank is involved in each payment. In this case, the bank maintains a database with all spent cash, and immediately verifies whether it is doublespent. Doublespender identification in offline systems is more involved since the bank can detect it after the fact. One solution is to implement an electronic *wallet with observer*, a hardware device which can prevent from any copy or modification attempts. However, this solution requires tamper-resistance.

Most proposed solutions construct cash systems in such a way that the identity of the user is known, and any double-spending attempt would lead to identification after the fact. To realize this without sacrificing the anonymity, advanced cryptographic techniques are applied. The desired mechanisms must exploit the fact that two deposits with the same coin reveal the information required for the purpose of identification, but, this must be infeasible with a single payment. One way to implement this is to use the *challenge and response* principle as proposed in Chaum, Fiat, Naor³⁰⁹ for the first time. There, in each payment, the receiver challenges the payer by asking a question. The payer has to correctly answer by sending a response. There are different ways proposed to realize this³¹⁰. For this, the payer secretly encodes her identity into the coin during the withdrawal to be verified by the bank. The payer remains anonymous as long as there is a single response in the payment for a coin. However, a further payment with the *same* coin will generate a second response, and the bank can use the two different challenges and responses to recover the encoded identity later at deposit.

Since Chaum's publication of blind signature and its deployment for constructing electronic coin systems, there have been many proposals for such systems, particularly offline systems³¹¹. They differ in their underlying cryptographic systems, the properties they offer, and their efficiency.

Electronic coin systems mentioned before are not transferable since a coin can only be spent once before depositing it. For a coin to be transferable, it must also contain the blinded identifying information about all its owners. This means, however, that the coin grows in size³¹².

In the past, there have been some achievements to implement electronic cash systems. Here, we will mention a few of them:

- A well-known product for a coin system is *ecash* conducted by DigiCash. It realizes an online coin system with payer anonymity and non-anonymous accounts based on the ideas of David Chaum³¹³.

³⁰⁹ See: Chaum, Fiat, Naor (1990).

³¹⁰ See: Franklin, Yung (1993); Brands (1993b).

³¹¹ See: Okamoto, Ohta (1990); Ferguson (1993); Brands (1993a/b); Brands (1995); Okamoto (1995).

³¹² See: Chaum, Pedersen (1993a).

³¹³ See: Chaum (1984/1985/1989).

- One of the most efficient offline coin systems is proposed in Brands³¹⁴. It is based on the blind signature scheme introduced in Chaum, Pedersen³¹⁵, and offers unconditional payer anonymity. An European research project on developing anonymous offline electronic cash was *CAFE* (Conditional Access for Europe).
- Another example for an electronic cash system is *NetCash*³¹⁶. *NetCash* is an online payment system using identified coins, i.e., coins are tokens with serial numbers signed by the bank. It uses symmetric and asymmetric cryptography to establish secure channels. Since *NetCash* uses identified coins, it cannot provide anonymity, at least not to the degree as other coin systems provide.
- *Mondex* is a smart card based solution for which most technical information was not published. Users load their cards at *Mondex* ATMs. For payments the money is transferred from one card to another through an appropriate device and no online verification with the bank is needed.

IX Escrowed Cash Systems

Anonymous cash systems have also a dark side. The anonymity property can be misused for illegal transactions and criminal activities such as blackmailing and money laundry (see also Froomkin/ Sander, Ta-Shma³¹⁷). This was first addressed by Solms, Naccache³¹⁸ where they consider the problem of blackmailing the bank also known as *blindfolding*. Since then effort has been put into designing *anonymity-revocable* payment systems, also called *fair* or *escrowed* cash systems³¹⁹. In such systems, one or more trusted third parties (called trustees) can help the bank to revoke the anonymity, in case of justified suspicion.³²⁰ A well-structured survey on such systems can be found in Petersen, Poupard³²¹. The role of the trustee can be *active* or *passive*. An active trustee is involved in registration (opening an account) or in every withdrawal protocol, or even in payment. Systems with passive trustees³²² are more practicable, since the trustee

³¹⁴ See: Brands (1993a).

³¹⁵ See: Chaum, Pedersen (1993a).

³¹⁶ See: Medvinsky, Neuman (1993).

³¹⁷ See: Froomkin (1996); Sander, Ta-Shma (1999).

³¹⁸ See: Solms, Naccache (1992).

³¹⁹ See: Brickell, Gemmell, Kravitz (1995); Camenisch, Maurer, Stadler (1996); Camenisch, Maurer, Stadler (1997); Camenisch, Piveteau, Stadler (1996); Davida, Frankel, Tsiounis, Yung (1997); Frankel, Tsiounis, Yung (1996/1998); Jakobsson, Yung (1996); Solages, Traoré (1999).

³²⁰ For instance, the specific mechanism applied against user blackmailing is *coin tracing*. It is similar to tracing serial numbers of banknotes. The trustee is given specific withdrawal transcripts which the bank has stored during the withdrawal protocol. The trustee is asked to retrieve information to be used by the bank or the merchant to recognize the spent coins. This helps the authorities to find the destination of the extorted money.

³²¹ See: Petersen, Poupard (1997).

³²² See: Camenisch, Maurer, Stadler (1996); Davida, Frankel, Tsiounis, Yung (1997); Frankel, Tsiounis, Yung (1996/1998); Solages, Traoré (1999).

is not involved in any of the system's protocols. The trustee is present passively through its public and authentic parameter (e.g., public key). The common approach is that the payer encrypts some information using the trustee's public key and proves to the bank — and in some approaches to the merchant — that the content of the encryption or a transformation of it will appear in the coin, and thus, reveals the required tracing information. However, for a large class of existing proposals for anonymity–revocable cash the problem of a blackmailing user can be solved without involving any trustee^{323, 324}. Note that the mentioned proposals cannot prevent blindfolding protocols. Examples of systems with mechanisms against such attacks are Fujisaki, Okamoto/ Jakobsson, Yung/ Petersen, Poupard³²⁵.

An alternative but rather inefficient approach for designing anonymous electronic cash systems with tracing capabilities is introduced in Sander, Ta-Shma³²⁶. It is an auditable system and requires no blind signatures. The security of the system relies on the ability of the bank to maintain the integrity of a public database.

X Micropayment Systems

With the rapid growth of open communication networks, they will be increasingly used for delivering low-valued (e.g., less than 1 Cent) information goods and services to a large number of consumers. Examples for such applications are browsing web pages of online magazines and newspapers, querying databases, downloading music or video streams, among others. Most of the previously presented electronic payment systems are not really adequate for handling micropayments due to their high processing costs, e.g., because of computational and communication overhead.

Some of the proposed micropayment systems have already been tested in practice, but so far, they did not achieve a broad market acceptance. The experiences made so far may be valuable for the development of new successor generations of micropayment systems.

The model of some micropayment systems involves an additional party called *broker*. A broker can be considered as an intermediary among payer, merchant, and banks. It is used for functional purposes, e.g., to introduce flexibility for payers by exchanging merchant-specific currencies or by allowing them to be in contact with many merchants without being required to open accounts at each merchant. For the sake of simplicity, we consider brokers to belong to the financial infrastructure. Thus, we do not differentiate brokers from banks.

³²³ See: Pfitzmann, Sadeghi (2000).

³²⁴ More concretely, instead of a trustee, the blackmailed person herself reveals the required information to trace extorted coins without compromising any of her secrets.

³²⁵ See: Fujisaki, Okamoto (1997); Jakobsson, Yung (1996/1997); Petersen, Poupard (1997).

³²⁶ See: Sander, Ta-Shma (1999).

There is a relatively large body of literature on micropayment systems. As mentioned before, these systems do not offer all desired properties (e.g., anonymity) of some electronic macropayment systems. Well-structured categorization and analysis of many of these systems are given in Lipton, Ostrovsky/ Peirce/ Weber³²⁷. Here, we categorize micropayment systems according to their property whether transactions in payment systems are either dependent on some probabilistic decisions (see Section V).

X.1 Payment Transactions without Probabilistic Decisions

Here, we consider those micropayment systems whose execution is not dependent on the outcome of random experiments. The systems to be considered here can be distinguished according to the degree they use costly computations, mostly resulting from cryptographic computations. Certain categories of cryptographic primitives (symmetric cryptography, asymmetric cryptography) cause different costs.

A system which can operate with very little cryptography is *MilliCent*. *MilliCent* is a micropayment system which uses special forms of electronic coins called *scrip*³²⁸. Scrip can be understood to be similar to a pre-paid calling card, or a debit card specific to a merchant. Scrips are merchant specific, i.e., they can only be spent at their corresponding merchants. Payers can buy larger amounts of scrip in a single transaction by using an appropriate macropayment system. The bank maintains accounts of payers and merchants. The main security problem of this type of micropayment schemes is overspending, and proposed measures such as online verification, or maintaining blacklists about cheating users by all concerned merchants and banks are expensive. *MilliCent* offers three different protection levels. The strongest protection level applies symmetric cryptography with scrip-based exchange of a shared key for the provision of security, e.g., to deal with scrip forgery and privacy in communication. The second level does not use symmetric cryptography whereas the lowest level provides no security at all. There are other systems reducing computational effort by exclusively using symmetric cryptography in order to allow small-value transactions. In these systems, symmetric cryptography is mainly used for purposes such as authentication and authorization of fund transfers between the payer's and the merchant's account, i.e., the payer authorizes the payment order by using the secret key which she shares with the bank. Since the merchant does not know the secret key of the buyer, he is not able to forge purchase details or to obtain information since it is exchanged in an encrypted way. Here, the payment order is just an instruction for the bank to debit the payer's account. Note that in these systems no coin-like monetary values are used or stored, and therefore, no overspending is possible. As mentioned before, these systems are online and are inefficient if used frequently. Examples are the online payment system of Tang³²⁹ and *Cyber-*

³²⁷ See: Lipton, Ostrovsky (1998); Peirce (2000); Weber (1998).

³²⁸ See: Glassman, Manasse, Abadi, Gauthier, Sobalvarro (1995).

³²⁹ See: Tang (1995).

Coin which was developed as an extension to *CyberCash* (see O'Mahony, Peirce, Tewari³³⁰). Another advantage of such systems is that payer system crashes do not result in monetary loss for her. Unfortunately, the payer's privacy is not protected since the bank gets aware of the payer's commercial relationships.

Other payment schemes allowing small- and low-value payments use asymmetric cryptography, e.g., to generate digital signatures, even if this requires higher computational effort. These systems use asymmetric primitives for payer authentication and payment authorization. Examples for such systems are *NetBill* (see Section VI) and *NetCent*³³¹. *NetCent* improves *MilliCent* mainly in the sense that *NetCent* scrips are not merchant specific and can be directly transferred from one merchant to another. Overspending is not possible since the payment order is just an instruction for crediting the payer's account by subtracting the corresponding amount from the current balance.

MiniPay is another micropayment system which applies asymmetric cryptography with its focus on web applications. It allows to "pay a Cent per click"³³². The idea of *MiniPay* is to save costs for payment order transmission by attaching it on the payer's *http* information request (GetURL). It is proposed that the typical bank's part are played by an Internet service provider and an Internet access provider. Each payment order sent to the merchant is signed by the payer. Payments will be accepted if they are within a given monetary range valid for a specific period of time, e.g., a day. This limit is contained in the payer's public key certificate. Merchants collect the payments obtained from their customers before they forward them for deposit reasons in an aggregated way. While collecting, no verification other than that of signatures is performed. This reduces communication costs as they usually arise in online payment systems. On the other hand, this allows overspending; it is possible that a payer spends money up to its limit at many merchants within the corresponding period. Furthermore, all signatures generated by the payer have to be transferred and verified for deposit which entails costs for communication and computation. Another system similar to *MiniPay* was proposed in Blaze, Ioannidis, Keromytis³³³.

There are micropayment systems in which merchants do not need to forward all collected payments to the bank, though, they allow the bank to implicitly verify all the payments at deposit. A class of micropayment systems providing this property is based on *one-way chains*.³³⁴ The first proposal for such a payment system was given in Pedersen³³⁵. The basic idea is to implement micropayments with a one-way chain introduced in Lamport³³⁶. Let f be a one-way

³³⁰ See: O'Mahony, Peirce, Tewari (1997).

³³¹ See: Poutanen, Hinton, Stumm (1998).

³³² See: Herzberg, Yochai (1997).

³³³ See: Blaze, Ioannidis, Keromytis (2001).

³³⁴ These systems are also called *coupon-based* systems.

³³⁵ See: Pedersen (1997).

³³⁶ See: Lamport (1981).

function (e.g., a secure one-way hash function).³³⁷ The payer computes the value $w_n := f^n(w_0)$ where w_0 is a random value, and f^n denotes n iterations of the function f , i.e., $w_0 = f^0(w_0), w_1 := f(w_0), w_2 := f(w_1) = f^2(w_0), \dots, w_n = f^n(w_0)$. The chain elements w_i are used by the payer to make micropayments of a fixed value v . As an example, consider a payer sending subsequently $n = 10$ chain elements to the same merchant where each element has a value of 1 Cent, she gives him a total value of 0.1 Euro. Before starting the payments, the payer commits to the entire chain by signing the last element w_n of the chain and sends it to the merchant.³³⁸ After the merchant has verified the signature, each successive payment is carried out by revealing $w_{n-i} := f^{n-i}(w_0)$ for the i -th payment to the merchant, i.e., the chain of hash values is spent in reverse to the way it was generated. The merchant stores the payer's signature on w_n and also the last obtained value w_{i-1} to be able to verify the next micropayment w_i . To clear the payments, the merchant presents the signature on w_n and the last obtained chain element w_{n-k} for $(0 < k \leq n)$ to the bank. Note that beside the signature on w_n , only one chain element has to be transferred to the bank. The bank can re-calculate the relevant part of the initially generated hash value chain and verifies whether $f^k(w_{n-k}) = w_n$ holds. After positive test, the bank credits the merchant k times the value of a chain element, e.g., k Cents. Other similar coupon-based micropayment systems with hash chains are *PayWord*³³⁹, *micro-iKP*³⁴⁰, *NetCard*³⁴¹ and *PayTree*³⁴².

A further scheme based on a specific form of electronic coins is *MicroMint*³⁴³. *MicroMint* coins can be spent at any merchant. In the model, the coins are minted by a bank and sold to the payers. After a payment, coins are redeemed to the bank by merchants. In contrast to other electronic macropayments, coins do not represent the signature of the bank on a value since signing and verifying a coin would be computationally expensive. Instead, they propose a method for minting and verifying coins based on n -collisions of one-way hash functions.³⁴⁴ To be able to mint and verify coins efficiently, the authors propose that the bank must be provided with special-purpose hardware devices to be able

³³⁷ Informally, a function from a set X to a set Y is called one-way function if $y := f(x)$ can be computed efficiently but it is infeasible to compute x from y .

³³⁸ The payer may also sign other data such as the value of a chain element, the merchant's name, or a sequence number to avoid replay attacks.

³³⁹ See: Rivest, Shamir (1997).

³⁴⁰ See: Hauser, Steiner, Waidner (1996).

³⁴¹ See: Anderson, Manifavas, Sutherland (1997).

³⁴² See: Jutla, Yung (1996).

³⁴³ See: Burstein (1998); Rivest, Shamir (1997).

³⁴⁴ More precisely, a coin is a n -way hash function collision. Let f be a one-way function. An n -collision occurs, if there exist n different values x_1, x_2, \dots, x_n which are mapped to the same value by the function f , i.e., $f(x_1) = f(x_2) = \dots = f(x_n) = y$. A coin will then be (x_1, x_2, \dots, x_n) . However, finding such collisions is computationally not easy. Note that f cannot be implemented by usual one-way hash functions, e.g., MD5 or SHA-1. For those it is assumed that finding collisions is infeasible.

to perform the hashing required for minting coins, i.e., finding collisions. Such hardware and several other measures are required to prevent large-scale forging of coins. Moreover, the scheme offers no means against doublespending and can only use blacklisting offenders by keeping track of overspent coins from payers and merchants.

X.2 Payment Transactions with Probabilistic Decisions

As we have seen in previous sections, electronic (micro)payment systems are either online and involve a third party in each transaction for verification against overspending, or they are offline and can detect overspending after the fact. To reduce the number of transactions, a new class of micropayment systems based on *probabilistic decisions* has been introduced. In this context, there have been two different approaches, namely, probabilistic *verification* and probabilistic *payment*. Examples for the former approach are *probabilistic audit*³⁴⁵ and *probabilistic polling*³⁴⁶. The basic idea is that at purchase the payer gives signed payment orders to the merchant who decides only with a certain — rather small — *probability* to contact the third party (e.g., bank) for payment verification. The decision probability may be constant³⁴⁷ or proportional to the amount of the payment³⁴⁸. This idea combines the methods of online and offline payment systems to limit overspending while eliminating the need for verifying each payment. The shortcoming of these schemes is that doublespenders must be blacklisted, and all merchants must be informed and a revocation list must be maintained either at the merchants or at the bank. Another proposal using randomized audit in combination with hardware is given in Yacobi³⁴⁹. Also here, compromised smart cards must be revoked and the revocation list must be broadcasted to all merchants.

Next, we consider the probabilistic payment approach. One of the first proposals is given in Wheeler³⁵⁰. The basic idea is that for each micropayment the payer and the merchant interact according to a pre-determined protocol, e.g., the coin flipping protocol in Blum³⁵¹, so that with a small probability p this micropayment is selected, otherwise discarded. In other words, for each payment the payer has to pay a larger amount with probability p , and with probability $1 - p$, the payer pays nothing. For instance, if $p = 1/1000$ and the value of a micropayment should be 0.1 Cent, then, out of 1000 micropayments 999 will be discarded and 1 will be paid for 100 Cents on average. The advantage of this approach is that the bank requires to process only one single payment. Based on the ideas

³⁴⁵ See: Gabber, Silberschatz (1996).

³⁴⁶ See: Jarecki, Odlyzko (1997).

³⁴⁷ See: Gabber, Silberschatz (1996).

³⁴⁸ See: Jarecki, Odlyzko (1997).

³⁴⁹ See: Yacobi (1997).

³⁵⁰ See: Wheeler (1997).

³⁵¹ See: Blum (1982).

in Wheeler³⁵², Rivest proposes a lottery ticket based micropayment scheme³⁵³. The basic idea is that the payer issues a signed lottery ticket containing a *ticket value* and a *winning value* used later to determine the winner.³⁵⁴ If the payer has used the winning ticket and has given it to the merchant then he will be charged, otherwise not. A specialization using two hash chains is proposed in Rivest³⁵⁵ which avoids the usage of digital signatures. Some of the main shortcomings of this system type are (i) the payer is not bound to the outcome of the coin flipping protocol, and thus, can refuse to pay if the outcome is not in her interest, and (ii), no solution is proposed for the case the protocol is aborted at some stage which is known as the *fairness* aspect. Note that if this is allowed, then any of the involved parties may abort and restart the coin-flipping protocol changing the probabilities to its advantage. The payment system in Lipton, Ostrovsky³⁵⁶ uses the ideas in these papers and proposes solutions to the mentioned problems. More precisely, they present an authenticated coin-flipping protocol and prove its security. However, to achieve provable security they need to apply computationally expensive *zero-knowledge proof of knowledge protocols* where the user (merchant) proves to the merchant (user) that she (he) knows a certain value.³⁵⁷

Other probabilistic micropayment systems retaining the ideas of lottery tickets and *PayWord* are proposed in Micali, Rivest³⁵⁸. The authors address the main problems of micropayment systems such as *PayWord* and *Lottery Tickets* concerning efficiency and security, and propose solutions to remedy these shortcomings³⁵⁸. The main efficiency problem of *PayWord* is that the merchant cannot aggregate the micropayments of different users, i.e., the bank must also deposit a single micropayment which is not really viable due to the processing cost. The efficiency problem of *Lottery Tickets* relies in the interaction between the user and the merchant for selecting the micropayment. Moreover, in this scheme the payer has the risk that she may pay more than she should due to the probabilistic decision.³⁵⁹

³⁵² See: Wheeler (1997).

³⁵³ See: Rivest (1997).

³⁵⁴ The winning value can be a commitment, e.g., $y := h(x)$ where h is a secure hash function, to a value x which the payer should not learn at the time she issues the ticket. The commitment should be supplied by another party. The receiver has to know x in order to determine whether he is in possession of a winning ticket. In a concrete system, the merchant generates x , e.g., the outcome of an online coin-flip, and supplies the payer with y .

³⁵⁵ See: Rivest (1997).

³⁵⁶ See: Lipton, Ostrovsky (1998).

³⁵⁷ Loosely speaking, in a zero-knowledge proof of knowledge a prover proves to a verifier that she knows a secret value without revealing any information about this value.

³⁵⁸ See: Micali, Rivest (2002).

³⁵⁹ Note that although due to the law of large numbers the probability of such an event is small, the authors mention that this risk might have a great impact on the acceptance of such payment systems.

XI Past and Today's Practice

Many activities for establishing electronic payment systems into the market have been pushed by financial institutions and organizations. Thus, the availability of products has been mostly geographically bound due their spheres of activity. Many systems, which have been introduced, have already disappeared or have only reached a limited number of users. Furthermore, there is a considerable dynamic in this market. So, the situation may change between the time of this writing and publishing.

Here, we will restrict our considerations only to a small fraction of those systems which have been implemented as products — either still in use or presently not available anymore. Future needs concerning the availability of payment systems may bring some practical solutions back into the game. More information concerning various electronic payment systems can be found at <http://www.ex.ac.uk/~RDavies>.

DigiCash's product *ecash* was used by the American *Mark Twain Bank*, the Finish *Eunet*, and by *Deutsche Bank*, Germany, among some others. It was a pre-paid coin system based on *Chaum's* idea³⁶⁰. However, field trials with this system have been stopped, and the payment system is not provided anymore.

In the late 90s, *MasterCard* and *Visa* started to try pushing *SET* as an electronic credit card system into the market. Even if it promised better protection than sending credit card numbers over secured connections, *SET* was not really successful. Implementation and usage were too expensive for many merchants and payers.

PayPal is a rather successful payment system which allows person-to-person payments which became very popular. According to Punch³⁶¹, there have been more than 10 Millions of *PayPal* users in the United States in year 2001. This success is strongly related to its deployment in the *eBay* online auction system which became very popular. The auction business model exactly requires the person-to-person functionality that *PayPal* provides. Payer and payee have accounts at the *PayPal* provider. Payments are sent via emails. The payer sends an email to the provider and gives him the email address of the payee. Then, corresponding accounts are debited and credited. In the background, an ordinary credit card payment system is used for transferring money between a user's bank account and his *PayPal* account.

Paybox is a pay-now system that uses out-band authorization to authorize the payment. In the *Paybox* system, the authorization is given via a mobile phone, and thus it is not sent via the Internet. In a purchase, the payer sends his mobile phone number to the merchant who forwards this number together with the payment amount to the *Paybox* provider. Afterwards, the provider calls the payer in order to let her authorize the payment. The payer is authenticated by possession of the mobile phone and by typing-in some additional secret. After

³⁶⁰ See: Chaum (1983/1989).

³⁶¹ See: Punch (2001).

positive authorization, the *Paybox* provider requests the corresponding amount from the payer's account via a *debit order* payment system. Obviously, *Paybox* requires a mobile device, e.g., a mobile phone which has extremely high diffusion today. The provider at least learns about the relationship among payers and merchants, and also how much a payer spends at merchants.

XII Conclusion

In this work, we have given a survey on electronic payment systems. In the last years, there have been many proposals for electronic payment systems both in the industrial and academic area. However, many attempts to push these into the market unfortunately failed so far, but for their future, some conditions may change. Electronic payment systems seem to be promising in the future, especially those systems that allow payments over networks. When commerce with digital goods delivered over the Internet will evolve then secure electronic payment systems will become more and more relevant. New future applications in the area of information commerce, stimulated by the developments in digital rights management systems, will require comfortable and immediate payments. Many electronic payment systems as they are proposed by the academic community are still not applied and implemented in current products, although they provide users with much better security and privacy properties than systems that are often used today. In the past, lots of proposals have been criticized due to their inefficiency, but with the development of more powerful computer systems and networks these requirements become less dominating. Payment systems used today also consider security to some extent but they widely neglect privacy aspects. However, in practice providers promote their payment products by praising their security properties. Unfortunately, most customers are not really able to compare these products on their own by the information they are given.

Since the deployment of electronic payment products heavily depends on financial institutions and organizations focusing on national markets, there has been a lack of coordinated activities at an international level in this area so far. However, experiences made will be valuable for future decisions and developments.

From the today's perspective, there seems to be no question that electronic payment systems will evolve. Unfortunately, it is still impossible to say which system will be the future standard Internet payment system. Finally, this question will be answered by banks, merchants, governments, and also by the mass of normal users.

XIII Acknowledgement

We are grateful to M. Fuckard for many valuable comments and for his infinite readiness to help. Also many thanks to Michael Steiner for his valuable hints and for his efficient cooperation.

2.3.7 Mobile DRM

*Frank Hartung*³⁶²

I Introduction: The Need for Mobile DRM

During the last years, the mobile cellular networks have evolved from pure voice telephony networks to universal data networks. The so-called first generation of mobile networks, that means the analog systems like for example AMPS or TACS, provided circuit switched point-to-point connections between two users for voice services. The second generation, mainly known through the GSM system, provides additional capabilities for point-to-point data transmission, at comparably low bit-rates. However, with the evolution of second generation systems, visible for example in the GPRS technology, and with the introduction of 3G systems like UMTS, Internet technology like the use of IP protocols has been introduced into mobile networks, together with radio technology that provides higher data rates for the end user. Thus, evolved 2G and 3G systems offer possibilities and services previously only known from the Internet, and extend Internet access to mobile users. Mobile users now have access to Internet services like e-mail, web browsing, and to mobile services like multimedia messaging (MMS). MMS also allows exchange of messages to and from the Internet. In other words, Internet services become usable for mobile users, and mobile services like MMS become usable for Internet users. Thus, the Internet really extends to mobile users.

This trend is also visible in the ongoing evolution of mobile devices, which have developed from telephones to multimedia devices with color graphics displays, attached or built-in cameras, more processor power, polyphonic ring-tones, and pre-installed media players and streaming capabilities. Of course, with the development of network and device capabilities, services become more attractive, and the content transported over mobile multimedia networks becomes more valuable. Services delivering mobile content like ring-tones and logos for mobile devices generate considerable revenues already today. Mobile multimedia services delivering music, video clips, video streams, news services, sports news etc. will attract users even more in the future. Multimedia services are expected to increasingly contribute to the revenues in mobile networks, and content providers are aware of the opportunities of this additional distribution channel — especially since this is a channel that end users can access at any time, even when away from home and office.

A pre-condition for such services is, however, the protection of the content and digital assets transported to the end-user device using DRM technology. Therefore, DRM technology must be, and will be, implemented in mobile devices and mobile networks.

³⁶² Ericsson Research, Ericsson Eurolab Deutschland.

II Mobile DRM

While DRM is a general technology, and the problem to be solved a general problem of content distribution, there are some special aspects to be discussed and considered that distinguish mobile DRM from general DRM. These special issues include security aspects, interoperability, the importance of the super-distribution business model, and control over the transport network and its entities.

II.1 Mobile DRM vs. Internet DRM

The basic problem to be solved is the same for DRM in the Internet, in mobile networks, or in other data networks: controlled delivery of content, protection of digital assets, and enforcement of usage rights and permissions granted by an authorized entity (usually the content provider). However, there are some differences between for example the Internet and mobile networks that ease the introduction and use of DRM technology in mobile networks compared to the Internet.

First, the end-user devices have different properties. In the Internet, the hardware and software architecture of devices, that means of PCs, is public and well known. In fact one success factor of PCs has been this uniformity and openness of devices. Openness is not a disadvantage in itself, but in the PC case it unfortunately coincides with the lack of hardware or operating system security and DRM functionality that again helps protecting digital assets. Such lacking functionality are for example tamper-resistant memory areas or tamper-resistant software execution environments. This lack leads to the fact that DRM systems in PCs are likely to be more vulnerable to attacks and, in addition and due to the mentioned uniformity of devices, that one attack may be successful on different types or brands of devices — the “one hack fits all” threat. There are efforts to add tamper-resistance to PCs, *like the Trusted Computing Platform Alliance (TCPA)*³⁶³ *and the Palladium initiative*, but since this requires consensus between many stakeholders it is not likely to become a reality soon.

In contrast, the hardware and software architectures of mobile devices like mobile phones are typically not open, and different for each manufacturer. This is a consequence of the fact that the implementation of telecommunication devices is not standardized or uniform, only their interfaces to the network and other devices. Since manufacturers are free to change the architecture of their products, it is an easy exercise for them to add hardware and OS support for DRM, and it can be expected that we will soon see mobile devices that in fact have such DRM infrastructure or support functionality like for example tamper-resistant memory. Also, since devices from different manufacturers are different, the danger that an attack successful on one device would be successful on another device is low.

³⁶³ See: *Kuhlmann, Gehring* within this book on page 178.

Second, in mobile networks the end user is not anonymous, in contrast to the Internet. A mobile phone has to authenticate to and register in the network when switched on, and in general a phone can be associated with a user. Thus, the network operator can check the trustworthiness of a user (more exactly, of a device) before delivering content. The knowledge of the user identity, in other words the trust relation between mobile network operator and end user, can however also be exploited to make DRM systems more convenient for the end user, for example by using the mobile network billing functionality for charging of content and services.

II.2 Interoperability

Interoperability in general is an important issue in DRM: it is hardly acceptable if an end-user can access content from content provider A only using device X, and content from content provider B only using device Y, but device Y cannot use content from A. This is however the threat if different incompatible DRM systems are in use, be it proprietary or standardized systems. Some operators like NTT DoCoMo and KDDI in Japan have already used proprietary DRM solutions, but roaming between networks and services is difficult with isolated solutions. Lack of interoperability sets limits on possible growth. On a PC, the problem may be less severe, because a user can always download additional software and DRM modules. On mobile devices, this is in reality hardly possible, due to limitations of mobile devices, higher costs of mobile downloads, and usability and latency aspects. Therefore, the existence of a well-defined interoperable DRM solution that is widely supported is of even higher importance in mobile networks compared to the Internet and other fixed networks.

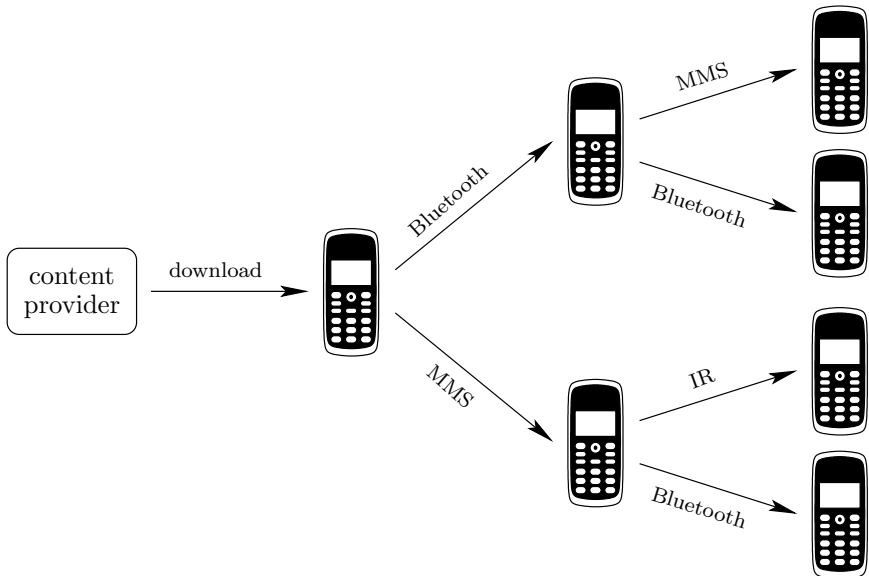


Fig. 1. The Super-Distribution Principle

II.3 Super-Distribution

An important aspect of DRM in an environment where users and devices meet physically is the support for direct super-distribution of protected assets. For example, if two mobile phone users meet, and one likes the ring-tone of the other's phone, it is a desirable feature that they can share the ring-tone by sending it from one phone to the other, via local connectivity like Bluetooth or Infrared (IR), or via the mobile network, for example by sending it as a multimedia message (MMS). Of course, the receiver must also acquire the rights to use the content. This super-distribution model allows peer to peer yet controlled distribution of content, and moves load away from the content server out into the network. The following picture shows the concept. It is regarded as an important feature of a good DRM system to support super-distribution.

III The OMA Standard for Mobile DRM

The Open Mobile Alliance (www.openmobilealliance.org), short OMA, is an open standardization body dedicated to defining an open standards based framework for mobile services and with a membership of more than 250 companies. OMA has defined a standard for Mobile DRM, and is currently defining a next, extended, version. This section explains the existing OMA DRM standard, and gives an outlook on its evolution.

III.1 History

In 2001 it was realized in the telecommunications industry that there existed an urgent need for a DRM standard that could be implemented in mobile networks and devices. At this point in time, no standard existed that seemed usable for mobile applications. Work had been done in MPEG, but it seemed not sufficiently applicable and mature. Thus, a group of seven companies (in alphabetic order: Ericsson, Motorola, Nokia, Openwave, Siemens, Sony Ericsson, Vodafone) proposed a DRM work item to the WAP Forum, which was eventually accepted. A similar work item had been started in 3GPP before. Due to planned standard releases, the release dates for the two work items in WAP Forum and 3GPP was significantly different: For WAP Forum it was mid 2002, while it was 3GPP Release 6, i.e., mid 2003, for 3GPP. Therefore, it was a widely accepted yet informal assumption that WAP Forum would standardize a first Mobile DRM release, sometimes called "DRM light", while 3GPP would standardize a second release, sometimes as informally called "full DRM". Both fora started their work, and WAP Forum finished its DRM standard (which will be described in more detail below) within less than 6 months. However, WAP Forum was then integrated into the newly founded Open Mobile Alliance. Shortly after, 3GPP decided to stop its DRM work item and to let OMA take over the work and existing requirements.

The reader should thus understand that the previous DRM standardization efforts in WAP Forum and 3GPP have been merged into the Open Mobile Alliance (OMA), which has published a first DRM release, and is working on a next release. All three efforts should be understood as one, now merged, activity.

A firm goal of the mobile DRM standardization was to produce an implementable and reasonable standard in a short time. Therefore, OMA has developed this standard in a bottom-up fashion: starting with basic functionality, but keeping the evolution path in mind, and developing the standard to a more advanced and secure version later on. This approach can be contrasted to the MPEG-21 approach, where the goal has been to define a very general and all-encompassing standard, and with the potential drawback of higher complexity and considerably longer time to finish the specification. Since mobile devices have a much shorter product life cycle than for example PCs, and since large numbers of new phones will be used with the introduction of 3G networks, it can be expected that OMA DRM will soon gain wide support among mobile operators and mobile device manufacturers.

III.2 OMA DRM Version 1

The OMA DRM standard has been released end 2002. The specification consists of three documents: one describing the general architecture³⁶⁴, one specifying the rights expression language (REL)³⁶⁵, and one specifying the DRM container format³⁶⁶. The specification concentrates on content packaging and expression of rights and permissions; it does not include strong security mechanisms to protect the content. This is clearly stated in the specification and based on the fact that OMA DRM version 1 concentrates on mobile specific content like ring-tones and logos (small images), not on high-value content like music or high-resolution images. Additional security and protection is to be provided by future versions.

OMA DRM stipulates three different levels or methods for DRM protection of content. They are called forward-lock, combined delivery, and separate delivery, respectively, and are explained in the following. An OMA DRM compliant device must support forward-lock. Combined and separate delivery are optional, but if a device supports them, it must also support forward-lock.

Forward-Lock

Forward-lock means that content is packaged into a special container format, called a DRM message. The content is not cryptographically protected, that means encrypted, but the DRM message format has an implicit restriction, namely that the DRM message and the included media object may not leave the receiving device after reception. It may be stored on the device and consumed without restrictions, but strictly only on that device. The DRM message

³⁶⁴ See: OMA-DRM.

³⁶⁵ See: OMA-REL.

³⁶⁶ See: OMA-DCF.

may be delivered to the device using e.g. the OMA Download mechanism. Figures 2 & 3 show the principle of forward lock, and an example of a DRM message containing a JPEG image.

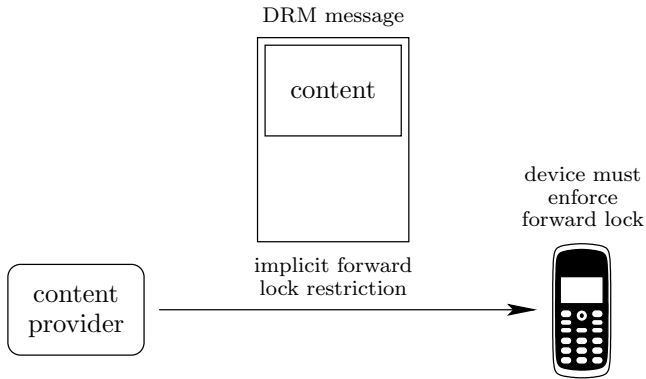


Fig. 2. The Super-Distribution Principle

```

HTTP/1.1 200 OK
Content-type: application/vnd.oma.drm.message;
              boundary=boundary-1
Content-Length: 622

--boundary-1
Content-type: image/jpeg
Content-Transfer-Encoding: binary

...jpeg image in binary format...
--boundary-1--

```

Fig. 3. The Principle of the DRM Message and its Use for Forward-Lock

Combined Delivery

Combined delivery extends the concept of forward lock by giving the possibility to define more fine-grained rights and permissions than the simple forward-lock restriction. As in forward-lock, the content is packaged into a special container format, the DRM message. Again, the content is not cryptographically protected, that means encrypted. However, in combined delivery a rights section is included into the DRM message, in addition to the media section containing the content. The rights section contains rights and permissions relating to the media object and specified using the OMA rights expression language (REL) which is discussed below.

The DRM message containing the rights and the content may be delivered to the device using e.g. the OMA Download mechanism. The Figure below shows the principle of combined delivery.

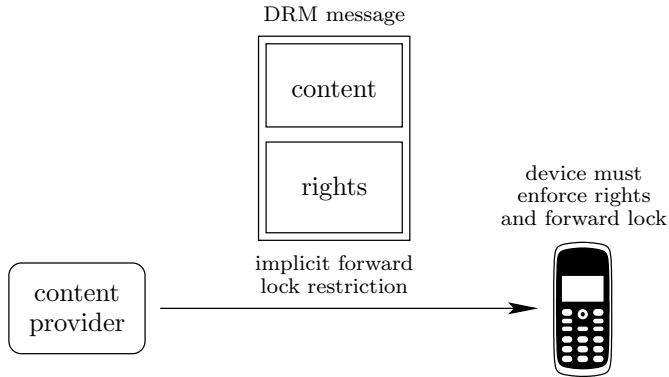


Fig. 4. Combined Delivery

Figure 5 shows an example of a DRM message containing a JPEG image, and with the permission for unlimited display. Note that the media object and the rights in the DRM message are bound to each other by a unique content identifier (URI).

Separate Delivery

As combined delivery is a logical extension of forward-lock, so is separate delivery an extension of combined delivery. As in combined delivery, it is possible to specify rights for media objects. However, rights and media objects/content are now transported separately, in two objects, compared to combined delivery where content and rights are transported in the same object. In the separate delivery method the media object is always encrypted and converted into the DRM content format (DCF). The encryption used is AES symmetric encryption in cipher block chaining mode and using 128 bit keys. Typically the DCF object is downloaded to the device using e.g. OMA Download, after which the rights object is separately delivered to the device using e.g. WAP push. The service is expected to indicate this behavior by using a special HTTP header that announces that a rights object is being pushed to the device. After receiving the pushed rights object, the device may use the included content encryption key to decrypt and render the media object according to the rights and permissions granted in the rights object. In an implementation, it should be taken care that the WAP push is directly sent to the DRM user agent in the receiving device and cannot be intercepted by other applications. The device may forward (super-distribute) the protected DCF file to another device. However, rights objects are not allowed to be forwarded, i.e. the receiving device must acquire rights for the media object from the rights issuing server. The following Figure shows the principle of separate delivery: DRM content and rights are transmitted separately, and the receiving device may forward the content object to another device. This may be done using local connectivity like Bluetooth or Infrared, or network connectivity like MMS. The second device cannot use the content, since it is encrypted. However, the content object contains some meta-data, in-

cluding a URL for rights object acquisition. The second device can then get the corresponding rights object, containing key and rights/permissions, and use the content accordingly.

```

HTTP/1.1 200 OK
Content-type: application/vnd.oma.drm.message;
              boundary=boundary-1
Content-Length: 1012

--boundary-1
Content-type: application/vnd.oma.drm.rights+xml
Content-Transfer-Encoding: binary

<o-ex:rights
  xmlns:o-ex="http://odrl.net/1.1/ODRL-EX"
  xmlns:o-dd="http://odrl.net/1.1/ODRL-DD">
  <o-ex:context>
    <o-dd:version>1.0</o-dd:version>
  </o-ex:context>
  <o-ex:agreement>
    <o-ex:asset>
      <o-ex:context>
        <o-dd:uid>cid:example001@DRMprovider.biz</o-dd:uid>
      </o-ex:context>
    </o-ex:asset>
    <o-ex:permission>
      <o-dd:display/>
    </o-ex:permission>
  </o-ex:agreement>
</o-ex:rights>
--boundary-1
Content-type: image/jpeg
Content-ID: <example001@DRMprovider.biz>
Content-Transfer-Encoding: binary
...jpeg image in binary format...
--boundary-1--

```

Fig. 5. The Principle of the DRM Message and its Use for Combined Delivery

The next example shows the structure of rights object and DCF for separate delivery. The right granted in the example is a one-time display right, that means a preview right.

After the preview in the example, the receiver could acquire a new rights object granting more rights, for example unlimited display right. Thus, the concept of separate delivery can be used for genuine preview and renewal of rights, without having to download the content again.

The OMA Rights Expression Language (OMA REL)

The rights expression language adopted by OMA is defined as a mobile profile of the Open Digital Rights Language (ODRL), version 1.1. The question of the choice of a REL was widely discussed in several other standardization bodies as well, for example MPEG. However, from a content provider point of view, the technology choice for a specific REL is not a very critical issue, as long as the REL supports the permissions and business models that content providers choose to apply. RELs can be translated to each other, and most RELs, including the OMA REL, are XML based and machine readable.

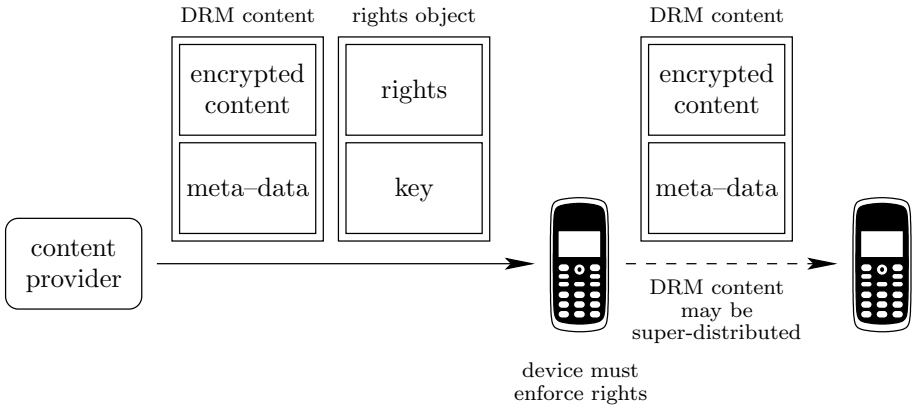


Fig. 6. Separate Delivery

In the OMA REL, rights are the collection of permissions and constraints defining under which circumstances access is granted to DRM content. The structure of the rights expression language enables the following functionality:

1. Metadata such as version and content ID
2. The actual rights specification consisting of
 - a Linking to and providing protection information for the content, and
 - b Specification of usage rights and constraints

Permissions that can be granted for content are “play”, “display” and “print”. Permissions can be constrained by “count” (i.e., number of uses) and “datetime” (start/end or interval). Permissions that are not explicitly stated are not granted. Rights can be encoded in textual, XML based format, or in compressed format using Wireless Binary XML (WBXML) encoding as specified in [REL]³⁶⁷. WBXML assigns short binary codes to the XML constructs. Thus, WBXML and XML can be translated into each other. The complexity of translation gains less data volume to be transmitted — an important aspect in mobile communications.

³⁶⁷ See: OMA-REL.

Security and Interoperability

OMA specifies packaging and signaling of DRM content and rights, but it does not specify how the standard has to be implemented. It relies on compliant implementations that provide security and DRM support in the hardware and the operating system. This seems to be a fair assumption in the telecommunications world, where only few renowned and trustworthy manufacturers build devices. More security will probably be introduced with the next version. Still, it can be expected that OMA DRM will soon gain support in devices and importance in the market.

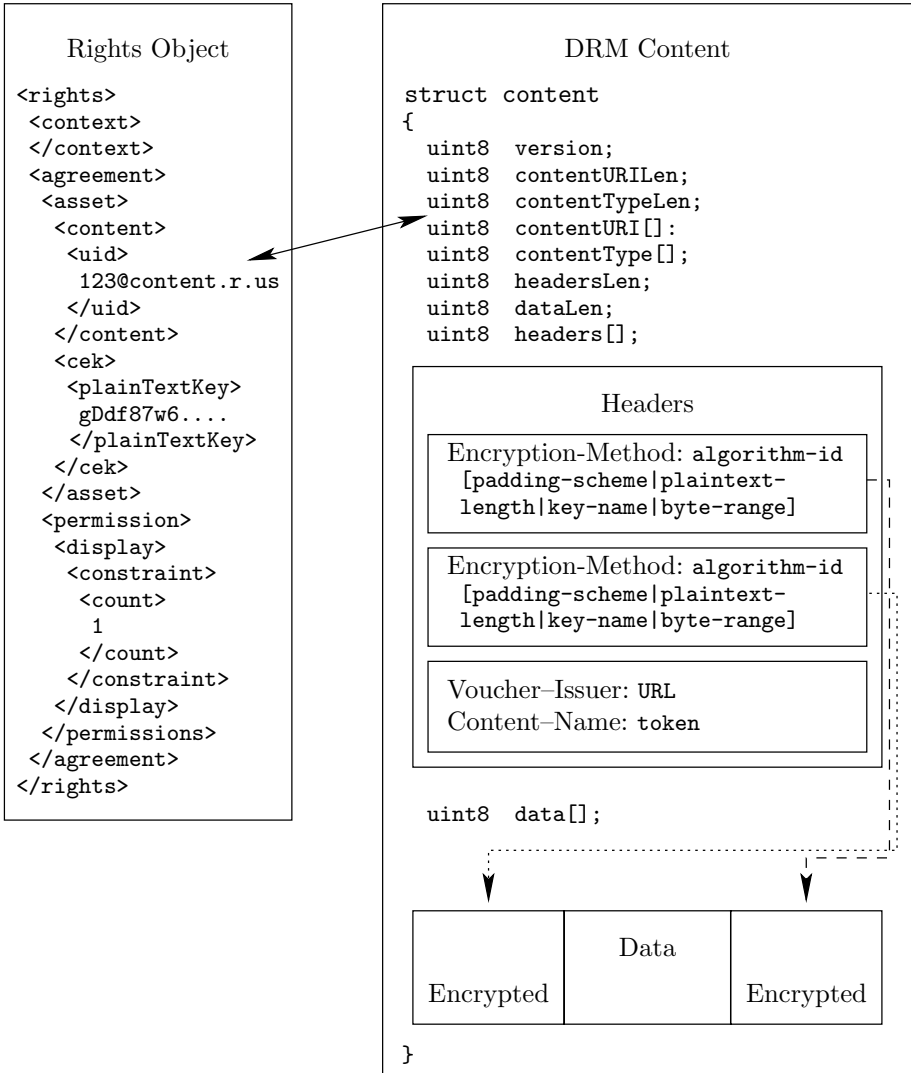


Fig. 7. Rights Objects and DCF in Separate Delivery

Architecture of an OMA Compliant DRM System

The standard does not specify a system architecture or required entities. However, five essential components are in practice needed in an OMA compliant DRM system:

- A packaging server that converts content (for example JPEG images) into DRM format (for example a DRM content container containing the JPEG image)
- A license server issuing rights and managing the content
- A content server hosting content in OMA DRM format.
- A payment function (or clearinghouse) clearing monetary transactions; this can be closely coupled to the mobile network billing system
- Compliant DRM clients implemented in devices.

Several or all of the server-side components above can actually be integrated into one server.

III.3 Standard Evolution: The Next OMA DRM Version

OMA is working on a next version of its DRM standard. However, according to the OMA rules, details of the ongoing work may not be disclosed at the time this book is being written.

IV Other Standards and Proprietary Solutions

As explained above, there exists no other usable open standard for mobile DRM. Inter-working of OMA DRM with Internet DRM standards such as MPEG-21 is desirable. From a content provider point of view the most important issue is probably a consistent specification of rights and permissions that are then expressed using different RELs, depending on the distribution channel.

The Bluetooth special interest group has defined protocols for audiovisual services over Bluetooth links. They have not specified an own DRM system, but signaling mechanisms to signal that content is protected by a higher-layer DRM system.

3GPP has been, and is defining standards for audiovisual mobile services like streaming and MMS. 3GPP is ready to adopt and adapt the OMA standards for such services.

Many proprietary solutions for DRM in general, but also for mobile DRM in particular, have been presented or announced, for example by companies like Lockstream, IBM, Intertrust, Microsoft, Sony, Realnetworks, Beep Science, NEC, and many others. Solutions from different vendors are in general mutually incompatible. Detailed properties and functionality are often not publicly disclosed. It can however be assumed that most solutions are based on similar principles: encryption of the content, specification and signaling of usage rules, cryptographic key management, and enforcement in a player or DRM agent in the device. Key

management and enforcement are usually the most critical components, and are typically kept secret to gain “security by obscurity”. It is known that security by obscurity is not a good and long-lasting way of keeping systems secure, but in practice it is still used to make re-engineering and hacking as hard as possible.

V Summary

Mobile networks have developed from voice networks to multimedia networks. This will become very obvious in the next years and with the adoption of evolved 2G, and 3G systems like UMTS. Mobile devices are also evolving to media devices with advanced audiovisual input and output capabilities. Accordingly, DRM technology is required to protect and control the transported content. Initiated by the lack of usable and open mobile DRM standards, the Open Mobile Alliance has developed a mobile DRM standard. In its available first version, the standard concentrates on content packaging, and the specification of usage rights and permissions. The standard provides different methods: forward-lock, combined delivery, and separate delivery. Forward lock defines a DRM container format for unencrypted content that implies the forward lock constraint. Combined delivery allows to specify more fine-grained rights using the ODRL-based OMA REL, like count-based or time-based display or print rights. Separate delivery adds some more security and super-distribution through encryption of the content using AES with 128 bit keys and separation of content and rights objects. Rights objects are usually pushed to the device. Content objects can be forwarded to other users, since they are unusable without the rights object containing the decryption key. The OMA standard has been defined bottom-up: starting with a basic version that shall be extended in a next version providing more security. This next version is under current development. It can be expected that OMA DRM will be implemented in devices soon and will become widely used for content distribution in mobile networks.

2.4 A Sample DRM System

Susanne Guth³⁶⁸

Abstract: The purpose of this chapter is to introduce a sample DRM system along with its basic functionalities, system components and internal information flow. An investigation of prevailing DRM systems shows that there are many variants of DRM system architecture, which makes it difficult to describe a ‘typical’ DRM system. However, what is typical in each DRM system is the basic functionality the systems provide. Therefore this chapter starts with a brief look at DRM systems from the functional perspective and identifies their basic functionalities, namely: *Content Provision, Content Safekeeping, Offer Creation, Content Preparation, Content Distribution, Booking, Payment, Authorization, and Content Consumption*. The functionalities identified are provided by DRM system parties such as the content provider, DRM platform, etc. A good deal of DRM systems can be described on the basis of these functions, although all these systems have different technical architectures. The sample DRM system described in the second section comprises all basic functionalities identified and displays a classic architecture in which the parties customer, DRM platform, content provider, and clearing house interact. The subsequent section describes the information flow through the sample DRM system. The chapter closes with an introduction of some commercial DRM systems with respect to their functionalities and system components; it finally addresses DRM system designs which differ architecturally from the sample DRM system. In some of these systems, additional parties come into play and assume responsibility for one or more DRM functionalities, thus changing the DRM’s architecture and information flow.

I DRM System Functionalities

A DRM system provides a trusted environment for the secure handling of digital content between contracting parties. Secure handling involves several functionalities, such as content provision, distribution, purchasing, and the delivery or rendering of digital content. The basic functionalities of a DRM system are similar, but the ways they are implemented vary, which means that DRM functionalities are executed by different system components with varying responsibilities and differing system architectures.

For example, let us assume a customer wants to access secure digital content. A license specified by the content provider defines the rights governing access to the content. Both the content and the license have to be delivered to the customer, and the rights have to be interpreted and executed. The implementation of this functionality can differ with respect to the following questions: Are the license and the secured content delivered to the customer together or separately? Are access rights interpreted and enforced by a mobile software agent or a secure viewer on the client’s PC, or possibly by a web server which regulates access to its realms? The variations mentioned result in various architectural styles in DRM systems.

³⁶⁸ Vienna University of Economics and Business Administration.

In this subsection, we introduce typical DRM functionalities, especially because naming the typical DRM functionalities helps us categorize and describe DRM systems. The functionalities introduced are used in the subsequent sections to describe a sample DRM system as well as alternative implementations of DRM systems which comprise these basic functionalities. Here the functionalities are arranged by their typical occurrence in a DRM system, although the existence and sequence of functionalities may vary from system to system.

- *Content Provision*: Content providers who decide to distribute electronic goods via a DRM system have to make the content available to the DRM system in some form. This initial functionality is called *content provision*. It is possible to distinguish whether the content is provided by the rights holder directly or by other DRM systems which act on behalf of content providers. Content provision also includes the delivery of content metadata, e.g., workflow metadata, metadata on security, and product metadata for content discovery. Metadata provision could be classified as an extra functionality. Some DRM systems do not consider content provision to be a base functionality and assume that content is simply available on the DRM platform.
- *Content Safekeeping*: Content safekeeping (or administration) deals with making the content available to the DRM system. Typically, this functionality merely supports the secure storage of traded content.
- *License Phrasing or Offer Creation*: Content provision is typically followed by offer creation (also called license phrasing). A license contains the terms and conditions, also called usage rights, which regulate content usage. The license phrasing functionality provides a means for the content provider to specify these terms and conditions.
- *Content Preparation*: In content preparation, the content is transformed into a secure, tradable format. The result of this process is a format called a *secure container*. The form of these containers varies in the different DRM systems. A variety of security technologies are used to create containers, and their ingredients vary from system to system. For example, in some systems the access rights are transported separately from the content. To learn more about DRM security mechanisms³⁶⁹.
- *Content Distribution*: Once the content has been prepared for trading, it has to be delivered to the customer. This includes content promotion as well as the provision of distribution channels.
- *Booking*: The booking functionality provides services for the customer to purchase content or, more precisely, to purchase usage rights for content. Booking or purchasing the digital product results in a contract between the content provider and the consumer. The contract should have an exchangeable and standardized format, and ideally it should be written in a standard rights expression language (REL — see article by *Guth* within this book starting on page 101).
- *Payment/Clearing*: In a great number of contracts, the purchase of digital content requires a payment from the consumer to the content provider or to

³⁶⁹ See: *Spenger* within this book on page 62.

the DRM platform (acting as a proxy). The payment has to be executed according to the specifications in the contract. For this task, a clearing house is required which provides various payment methods (credit card, debiting, electronic cash, etc.), maintains accounts for all involved parties and facilitates the settlement of payments. The term 'clearing' is sometimes applied to royalty payments from the DRM platform to the content providers rather than the payment to the customer-side DRM platform. We use the term 'clearing' simply for the incoming payment to the DRM platform; disbursement to the content provider is currently not within the scope of this model.³⁷⁰

- *Authorization*: Once the payment has been settled, the customer is allowed to access the content by means of a *token*. The authorization functionality transmits this token to the customer. Please note that the token is not the specified license. For the purposes of this chapter, we will define the token as a technical means, such as a decryption key for the secure container, which enables the customer to use the content according to the license.
- *Content Consumption*: Content consumption provides mechanisms to access and render the content kept in the secure container. Typically, consumption is facilitated by a DRM client software on the consumer's computer.
- *General Functionality: Workflow Control*: As various components typically interoperate in a DRM system, each component requires the integration of a workflow mechanism to control and coordinate the sequence of tasks and activities in the workflow through a DRM system.
- *General Functionality: Security*: The DRM system processes crucial digital content and data that has to be protected at all times. The content and data have to be protected against various types of fraud, such as unauthorized access or the modification of rights information (licenses). The following security techniques are used in DRM systems.
 - *Encryption*: Most DRM systems use encryption to protect the data circulating in the system. For efficiency reasons, symmetric key algorithms are generally used to encrypt the digital content, while asymmetric key algorithms are used to generate digital signatures and to establish secure channels.
 - *Digital signature*: Digital signatures provide a means of verification, integrity checking, authentication, and non-repudiation. For example, digital signatures can be used in DRM system to evidence the integrity of a license (or digital contract).
 - *Watermarking*: Watermarks bind information directly to the content. Most watermarking technologies claim to be unremovable from the content (even after data compression), which enables the lasting identification of digital content. For more information on watermarking³⁷¹.
 - *Secure Container*: The secure container technique is used as a secure transport format for digital content. Typically, the container protects the

³⁷⁰ See: *Sadeghi, Schneider* within this book on page 113.

³⁷¹ See: *Petitcolas* within this book on page 81.

content from unauthorized access. Erickson³⁷² states that the role of secure containers (wrapper) is that of a mediator service. The wrapper can link to services such as the repository, authentication and authorization.

- *Public Key Infrastructure (PKI)*: PKI is the basic infrastructure for many security technologies. It is used to provide digital signatures, encryption and decryption services, secure transport channels, key registration, certificate issuing and revocation services, etc.
- *Proprietary Mechanisms*: Not all DRM systems use standard technologies to ensure system security. Some systems use proprietary mechanisms and processes, for reasons such as unsophisticated standards in a particular field or the fear that known technologies are easier to circumvent.

The design of the security concept can heavily influence the entire system architecture and information flow. For more information on security mechanisms in DRM systems, please see: *Spenger* within this book on page 62.

The above-mentioned functionalities are basic ones and can also be read as a list of requirements for a DRM system. In this context, we distinguish between basic and advanced functionalities in DRM systems. The payment of royalties has been classified as a basic functionality, although there are DRM systems in which payment is not an obligatory part of the transaction, e.g., educational projects such as Universal³⁷³ or COLIS³⁷⁴, both of which are brokerage platforms for learning resources.

Advanced functionalities in DRM systems include: Tracking of content (IPR services), content creation (bundling), interfaces to other DRM systems for interoperability, automated disbursement of royalties to content providers on the basis of licenses, etc. This list will be lengthened as new generations of DRM systems emerge.

Functionalities versus System Components. Other works in this field deal with the definition of DRM system components rather than functionalities; for example, Rosenblatt, Trippe and Mooney³⁷⁵ define a DRM reference architecture on the basis of standard components. In our view, it is easier to understand, evaluate, compare, and categorize DRM systems using a set of functionalities. Where functionalities describe the smallest unit of the DRM system (module), a system component comprises several functionalities. The functionalities introduced can be implemented in many different variants. Some might even be processed by hardware components; for example, the European pay TV contractor Premiere World uses smart cards to handle parts of its security process. In the next section, one of many possible implementations is introduced.

³⁷² See: Erickson (2001).

³⁷³ See: <http://www.educanext.org/>.

³⁷⁴ See: <http://www.colis.mq.au/>.

³⁷⁵ See: Rosenblatt, Trippe, Mooney (2002).

II A Sample DRM System

In this section, we introduce a sample DRM system based on the functionalities mentioned in the previous chapter.

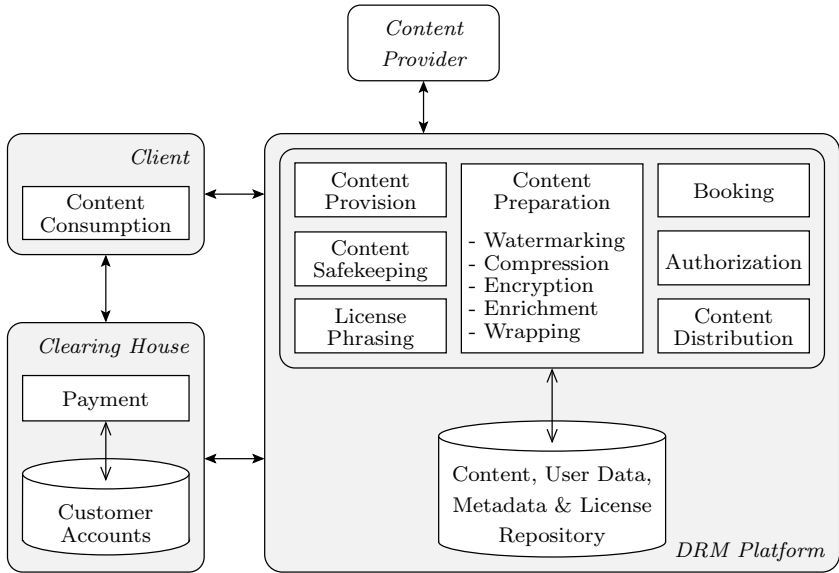


Fig. 1. A Sample DRM System

In this DRM system, the functionalities are assembled into components. For the purposes of this chapter, we define components as interoperating parties in a DRM system. The components in our example are the client (or consumer), the DRM platform, and the clearing house. As the content provider does not deliver any of the defined functionalities, s/he is simply a party who interacts with the system. Depending on the system's design, different or additional components which share DRM functionalities may also show up in a DRM system. The DRM platform is the key component which controls the DRM process in our sample system; this process involves interaction with content providers, consumers and the clearing house. The DRM platform provides the functionalities of content provision, offer creation, content safekeeping, content preparation, content distribution, and booking (cf. Figure 1). The payment functionality has been outsourced to a clearing house. Content consumption is supported by the client component of the DRM system.

III How Information Flows

This section describes the general flow of information through the sample DRM system. Although the functionalities are assigned to DRM components, there are implementation alternatives for each functionality. When describing the information flow through the system, we also try to address these alternatives.

1. *Content Provision.* First of all, content has to be provided by the rights holder (cf. Figure 2). Content provision can be technically implemented in many ways, for example by uploading to a content server or by sharing a folder on the provider's computer. An interface has to be provided for manual provision by content providers as well as automated provision by cooperating DRM systems. In order to facilitate interaction between cooperating DRM systems, a standardized interface is needed.

During the provision process, the content has to be protected from unauthorized access by security mechanisms, for example through a secure channel with the help of the secure socket layer (SSL) protocol, or in an encrypted format. The content metadata can be provided separately from the content. A graphical user interface should be provided for the manual input of metadata by content providers, or a standardized interface could be offered for the automated provision of content metadata records. One example of such an interface could be documents written in a standard language for product metadata (e.g., the learning object metadata (LOM) standard³⁷⁶ for the educational domain).

2. *Content safekeeping.* Once the content has been provided, it is stored in a secure environment in the content repository. Depending on the DRM system concept, the content is stored in plain format, or in a security wrapper (secure container). The metadata is stored in the metadata repository.
3. *License Phrasing or Offer Creation.* Content providers offer their content on certain terms and conditions. In our sample system, these conditions are not standardized but can be defined individually for each unit of tradable content. Specifying these terms and conditions can also be regarded as rights metadata provision. The provision of rights metadata results in an offer (also called a *license*). The offer creation functionality needs to be flexible and various business models should be supported. In practice, the content provider is guided through a menu where s/he is able to specify terms and conditions for any of his/her resources. The result of this process is a license written in a rights expression language (see article on page 101 in this book). Similar to product metadata, the license can either be provided by the content provider directly (personally) or by a cooperating DRM system acting on behalf of the content provider. In the latter case, an interface has to be provided to receive and exchange licenses formulated in an REL and to process them automatically. The necessary rules for DRM system interaction are defined in the work of Erickson³⁷⁷, who defined a general rights messaging protocol. The licenses are stored in the license repository.

³⁷⁶ See: LTSC (2002).

4. *Content Preparation.* The content then has to be prepared for distribution. In our sample system, this comprises the following steps:
- *Watermarking.* A watermark is added to the content. This watermark comprises metadata on the content and enables, for example, the identification of content. For more information about watermarks please see Petitcolas in this book — page 81.
 - *Compression.* The digital content is compressed into a manageable size, for example, from original memory-intensive picture representation to JPEG format.
 - *Encryption.* In order to protect the content against unauthorized access, the compressed content is then encrypted using a symmetric key mechanism.
 - *Enrichment.* The digital content is now enriched with metadata, such as licensing, product, security and workflow information.
 - *Wrapping.* The license and the encrypted content itself are wrapped in an additional security mechanism. The result of content wrapping is the secure container, which prevents unauthorized access throughout the content's life cycle.
5. *Content Distribution.* The secure container is delivered to potential customers through various distribution channels. The content can be promoted in peer-to-peer networks or sent directly to registered customers. Customers can exchange the secure containers privately in unstructured ways (superdistribution), or an e-commerce shop can serve as a distribution channel. The marketplace should have typical features, such as promoting, browsing and searching for content and providing purchasing information for the digital goods. An interface to an electronic commerce system which already provides these features could also be implemented. A number of DRM software solutions use such interfaces. The distribution channels should be able to serve various kinds of end devices, such as PCs, PDAs, cellular phones, etc.
6. *Booking.* When a consumer wishes to access content, s/he will need to acquire access rights by booking or purchasing the content. For this purpose, the DRM platform has to be contacted, a process which is invoked by DRM client software on the customer's PC. As this software is responsible for handling the secure container as well as rendering the content in compliance with the the terms and conditions, it is sometimes referred to as a *secure viewer*. The DRM platform's booking module receives the customer's access request and returns information on the payment process to the customer.
7. *Payment.* The customer then contacts the clearing house and initiates the payment process. The clearing house then balances the customer's and the platform's accounts and notifies the DRM platform of the payment. The electronic payment system *PayPal*, which is currently used predominantly by online auction participants, supports this payment procedure. However, other payment systems could be used as well. To learn more about electronic payment systems, please see Sadeghi and Schneider in this book — page 113.

³⁷⁷ See: Erickson (2001).

8. *Authorization.* As soon as the booking module receives the notification, it invokes the authorization process. The authorization module sends the content key (token) to the consumer. This content key complements the symmetric key with which the content is encrypted. The content is now ready for consumption. Please note that additional security mechanisms are applied to transfer the key securely, and that other identification mechanisms may be used at this point. In systems where licenses and content are delivered separately from each other, this is the point at which the license is received.
9. *Content Consumption.* Content consumption is executed by the client software, a secure viewer trusted by the DRM platform. It receives the key and proceeds to render the content, which comprises the following steps:
 - The customer invokes an *access request* for a certain unit of content. The secure viewer is able to process the request and handle the secure container.
 - The client then *verifies* whether access can be granted. For this purpose, the client has to check if the customer possesses the required token. If the token is available, the client software permits the rendering of the content. In cases where the token is missing or the license is distributed separately from the content, the client might initiate a task to obtain the license and/or token at this time.
 - If verification is successful, the content is *decrypted*. All information required for this process, such as the symmetric key which was just received or information on digital signatures, has to be available. Additional security information might be found in the metadata of the secure container.
 - The compressed content has to be *decompressed*.
 - Other functionalities, such as *quality control mechanisms* for ensuring content quality after encryption, compression, transmission and decryption of the digital goods, might be included at this time. Prior to rendering the content, the client software also has to execute a number of *security checks*. For example, it checks whether the secure container and its content have been manipulated during the distribution phase. The secure viewer verifies that the content identification number in the license is identical to the one in the watermark, etc.
 - Finally, the client *renders* the content in a way compliant with the license specifications (a process which is also called *rights enforcement*³⁷⁸), thus completing the DRM transaction.

However, the consumption of usage rights to a web site is handled in a different manner from the process described above. Access rights to a web site are typically enforced by the web server rather than the client, and usually no content has to be decompressed and encrypted first. This means that the consumption of digital goods can have various facets, and the DRM system must provide consumption mechanisms for all formats in which content is offered.

³⁷⁸ See: Guth, Koeppen (2002).

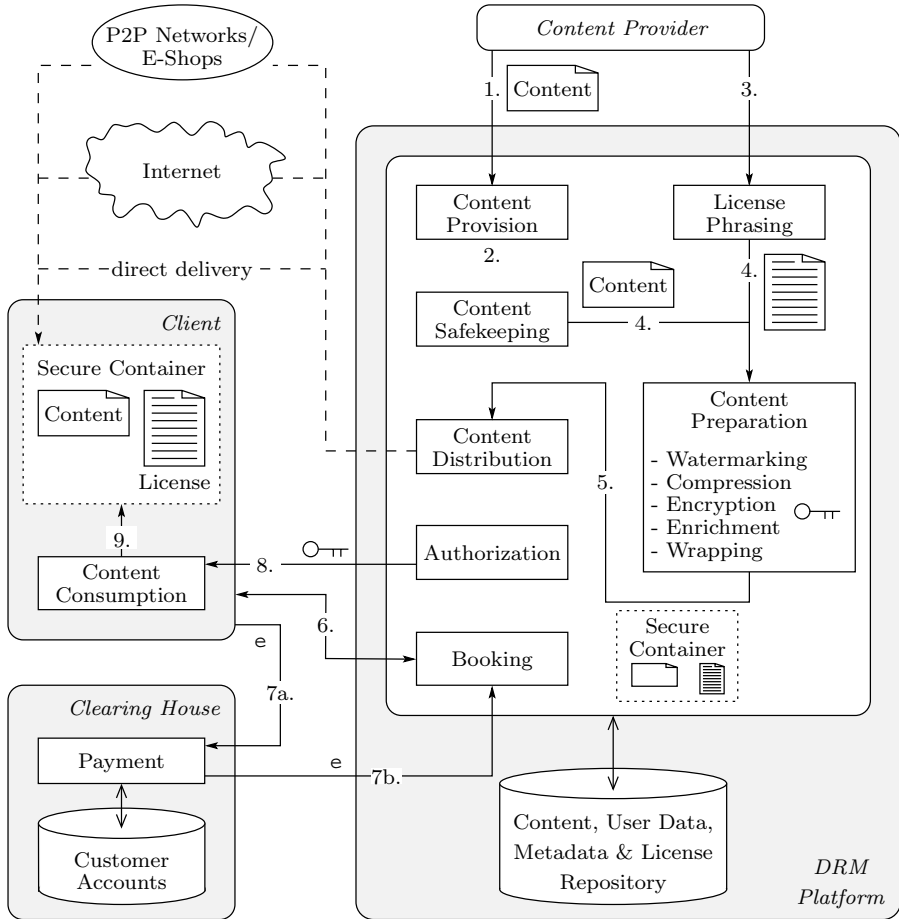


Fig. 2. How Information Flows through the Sample DRM System

In terms of security, the process described above only sketches a few mechanisms used in the field of DRM. The usage of other security mechanisms changes the information flow through the DRM system. The DRM system presented here assumes the availability of standardized or proprietary infrastructure for the identification of digital content (e.g., DOI), the standardized expression of meta-data, as well as infrastructure for security services. For simplicity's sake, we did not show the technical details of communication between the components. For more on these details, please refer to Erickson³⁷⁹, who describes a typical process flow through the DRM reference architecture introduced in [Rosenblatt, Trippe, Mooney]³⁸⁰ and investigates all necessary standards and protocols.

³⁷⁹ See: Erickson (2002).

³⁸⁰ See: Rosenblatt, Trippe, Mooney (2002).

IV Commercial DRM Products and DRM System Variants

The sample system in the previous section describes one classic form of a DRM system as well as one typical information flow (or workflow) scenario. However, as mentioned above, the DRM's basic functionalities can be shared by different or additional DRM participants, which results in alternative DRM systems with differing flows of information. In this section, we would like to give the reader an idea of the potential alternatives. For this purpose, we will introduce additional DRM system designs and current implementation approaches.

In the information flow described in the previous section, the license is bound to the content, while other DRM systems handle licenses separately from content. Both approaches have their pros and cons. The license which is bound directly to the content reduces the complexity of security and communication in the DRM system. The drawback is that the license or offer cannot be changed once it is issued and integrated into the secure container. This would cause problems in cases where content access conditions change and outdated versions of the secure container are still circulating. If the license is distributed separately from the content, an additional tamper-resistant connection to the DRM system is required in order to receive the license, but this approach makes the DRM platform very flexible in controlling, varying, and changing the terms and conditions for the digital content. This approach also allows the system to issue a license that applies to more than one unit of content. However, each of the two mechanisms has sensible applications, thus a DRM system should support both.

InterTrust has done pioneer work in the field of DRM. In describing InterTrust's DRM system, we will use the terminology and the graphic symbols from the previous sections (cf. Figure 3). In the InterTrust system design³⁸¹, the license and the content are handled separately from each other, both in a protected format. In this system, the licenses are administered by an additional, independent component called the Content Rights Server. The booking and payment functionality is delegated to an external e-commerce system. Once the customer has settled payment with the e-commerce system, the authorization module (called the Authorization Generator) sends an authorization (token) to the customer, who can then use it to retrieve a license for the purchased content from the Content Rights Server. Content consumption is then processed by the Rights—System Client.

The Windows Media Rights Manager³⁸² differs from our sample system in that the DRM platform does not host the booking service. The booking process is the responsibility of the clearing house. An additional booking module which challenges booking requests has to be installed in the clearing house component (called Microsoft's License Server). As Microsoft's system delivers the licenses

³⁸¹ See: Duhl, Kevorkian (2001).

³⁸² See: Microsoft — WMRM (2003).

separately from the content, the booking module is also responsible for delivering the license to the customer once payment has been made.

IBM's Electronic Media Management System (EMMS)³⁸³ distributes content and the associated rights together in a secure container. With the exception of its payment functionality, this system resembles our sample system. However, EMMS can be integrated into e-commerce systems which provide promotion, distribution and clearing services.

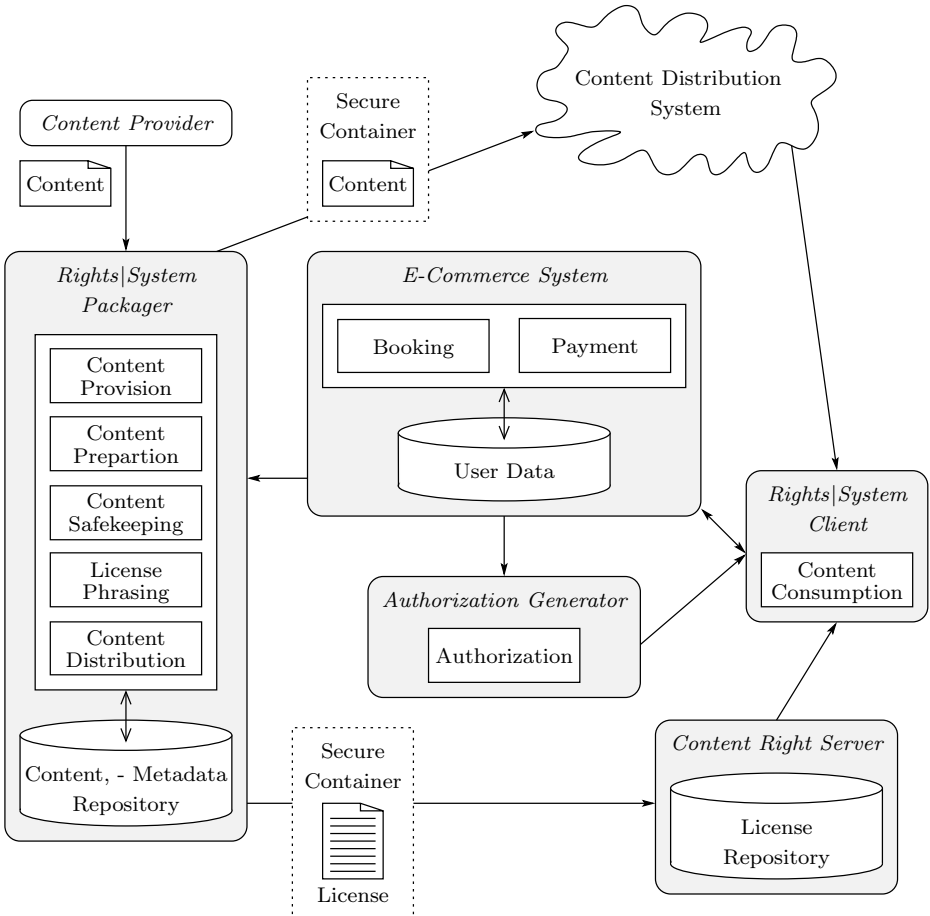


Fig. 3. InterTrust's DRM System

ADo²RA is a DRM system developed by Digital World Services³⁸⁴, which is part of the Bertelsmann Group. The system is designed with an additional component for almost every DRM functionality. It is worth noting that ADO²RA uses a

³⁸³ See: IBM-EMMS (2002).

³⁸⁴ See: DWS (2003).

sophisticated two-step solution for the authorization functionality. Content and rights are delivered separately, and instead of being transferred directly to the consumer, the rights tokens are sent to a *rights locker*. This is a central repository for tokens which is accessible to the customer from anywhere. Thus the customer can access the purchased rights from various locations, for example from the car, home or office, and from varying device types, such as mobile phones, PCs or PDAs.

The following approaches have not yet been developed as commercial DRM systems but introduce alternative technical approaches to the implementation of DRM systems.

A very generic, distributed system architecture is introduced in [Feigenbaum, Freedman, Sander, Shostack]³⁸⁵, where all functionalities are in the responsibility of a separate component, including content safekeeping, packaging and authorization. This approach is also designed with a rights locker for the storage of the customer's licenses. One prerequisite for the implementation of a rights locker is the separation of content and licenses (rights).

The work of [Konstantas, Morin]³⁸⁶ presents an agent-based approach in a DRM system developed as a prototype. In this approach, the content provider is responsible for provision and offer creation and delivers the content as well as the respective license to an agent platform via a secure channel. The agent platform then takes care of content preparation. The content and the license are wrapped together within an agent, the only application which can access the content – thus securing it permanently. The agent can then be released through the usual distribution channels. The agent also provides content consumption functionalities. In order to be executed on the customer's PC, the agent requires a suitable agent platform, for which Java technology was used in this prototype. Prior to accessing the content, the consumer has to consult the clearing house, which is responsible for booking and clearing. The customer obtains access (in the form of a token) from the clearing house and consequently does not get in touch with the content provider directly. The clearing house transfers payment and booking information to the DRM platform on a regular basis.

Please note that DRM systems do not necessarily have to deal with the delivery of encrypted content to the consumer. For example, in the case of an online newspaper which offers frequently updated content on web pages, a DRM system deals with granting access to those pages. Rights enforcement on the client side is of only minor importance in this context. In addition, DRM systems are not only prevalent in business-to-consumer relationships, but also in business-to-business relationships, where DRM is used to regulate trading among electronic brokerage platforms³⁸⁷.

³⁸⁵ See: Feigenbaum, Freedman, Sander, Shostack (2001).

³⁸⁶ See: Konstantas, Morin (2000).

³⁸⁷ See: Guth (2003).

2.5 DRM and Standardization — Can DRM Be Standardized?

*Spencer Cheng*³⁸⁸, *Avni Rambhia*³⁸⁹

Abstract: In this paper, we examine issues related to the standardization of DRM systems or, more generally, IPMP systems. Rationale behind the need for standardization, targets of standardization and some general guidelines for successful standardization are presented. Both successful and failed past standards are examined for lessons and strategy. Use cases, particularly from the point of view of fair use, are examined in this context. Currently active standardization activities, and technologies and techniques essential for their successful implementation are discussed in some detail. Finally, we summarize the discussion, and answer the million-dollar question — can DRM be standardized?

I Introduction

Several papers in this issue have already discussed DRM systems and various technologies included within. Intellectual Property Management and Protection (IPMP) systems are similar to DRM systems in intent. However, their scope of protection typically extends beyond use management of content to the monitored distribution and use of Intellectual Property (IP). Such IP can certainly be content, but can also include software programs or modules, transmission bandwidth, lyrics or music within the content, specific images within the content, specific resolution renderings, and so forth. From the point of view of standardization, therefore, IPMP has a wider scope of potential applications and technology. Nevertheless, considerations for both DRM and IPMP systems are similar, and we shall use the two terms interchangeably in the discussions that ensue³⁹⁰. In general, IPMP issues are considered in the MPEG and related worlds, while DRM is the main focus in publishing and business arenas.

II Standardization in DRM — Why Bother?

Before attempting to answer a question, it is sometimes worthwhile to ask whether the question needs an answer in the first place. Given the difficulty of creating a workable DRM solution, let alone a standardized one, why would one want to spend valuable time and effort to attempt standardization? We contend that standardization is essential to establishing the economies of scale that will make digital content and IP distribution a viable and profitable business. Non-standardized consumer services almost always cause excessive market

³⁸⁸ Morphbius Inc.

³⁸⁹ Eyemail Technology, Inc.

³⁹⁰ The emphasis of this paper is the standardization of B2C (business to client) DRM systems. B2B DRM systems are related to B2C DRM systems, but are governed by significantly different usability and liability considerations. They will not be considered here.

fragmentation that usually do not allow for an economy of scale to evolve, thus resulting in uneconomical demand.

The Cable-TV market bears elegant witness to the need for, and benefits of, standardization. The conditional access (CA) standard allows any authorized provider to send protected content to a single, largely standard set-top box for descrambling and rendering. Consider the case where no such system existed. For each major studio, or perhaps for each major group of channels, each home would have required at least a separate box, and possibly cable line, to unscramble the content. The cost overhead would have been extremely high, seriously affecting the deployment and popularity of cable TV.

The same considerations hold for the distribution of digital media. Unless DRM systems are standardized, users will, at the minimum, be required to have separate players for media from separate owners, even if the media format were to be the same. Imagine having one music player for music from Universal, and another player for music from BMG. Not to mention several others for each of the garage bands you enjoy listening to. Would you rather do that, or simply rip and burn music to a generic MP3 format, even though something in the back of your head whispers that ripping is somewhat illegal?

Unauthorized copying of digital content is sharply unlike normal theft for one major reason: The “theft” of a digital copy doesn’t deprive the original owners of their own copy. Hence normal ethical considerations about theft don’t provide a real deterrent. On the other hand, users value and desire easy, legal access to digital content. Well-built, standardized, usable DRM systems are the key to creating a win-win situation a.k.a. the MPEG-2 revolution. Users can get and play content easily and economically, the content owners and distributors are able to satisfactorily monetize their content, equipment makers can invest in improved lines of products knowing that the market is dependable, and everyone is happy.

So there are some truly important reasons to consider the question of standardization of DRM. The next section takes a brief look at the anatomy of a DRM system, and discusses targets of standardization.

III Anatomy of a DRM System

Several earlier papers have discussed the various components of a DRM system, from publishing to transfer, service and playback components. We therefore simply re-list them here for convenience:

1. *An identification mechanism.* Identifies, exactly, the digital item or piece of IP that is under transactional consideration. Unless an item can be unambiguously identified, it usually will not be bought and will be difficult to sell or track. Identification is sometimes extended to include “searchability identification”, i.e. data to help locate the item when searched using keyword, genre, similar media or other such criteria.

2. *A secure transmission and storage mechanism.* Typically involving obfuscation or encryption of some sort, this also contains information regarding the structure of the encrypted package. Sending a digital item in the clear, outside such a mechanism, is a very high-risk proposition.
3. *An ownership tracking mechanism.* Typically achieved via watermarking, this is the digital equivalent of a logo or copyright statement. When securely embedded, it can be used to prove and maintain ownership. Such markings are also often used to track usage and distribution in more benign environments such as radio broadcast or advertisement monitoring.
4. *A rights expression mechanism.* Often considered to be the crux of any DRM system, this is how rights and responsibilities pertaining to the use of the digital item are described. In many cases, these considerations also include the level of security required in the player that will render the digital item.
5. *Authentication mechanisms.* These are the digital equivalents of presenting a driver's license or passport and visa papers, depending on the seriousness of possible identity fraud. Primarily used for establishing trust and confirming identities, these are the basis for the trustworthiness and indemnification of a DRM system. Authentication in the form of digital signatures is also required as part of data integrity verification.
6. *Payment networks.* While these constitute the financial lifeblood of the entire DRM infrastructure, these are also very well defined and well established worldwide. Hence, despite their key importance, we shall take them for granted without discussion.
7. *The secure player.* By far the most important part of the overall DRM setup — this is also, unfortunately in our opinion, the least considered or understood. All the security in the world means nothing if the rendering platform is unable to or does not reliably and predictably enforce, enable and guarantee behavior in accordance with expressed and implied rules and policy. Furthermore, users are usually rather enamored of their players and such equipment often involves significant personal expenditure. Therefore, they are rather unlikely to want to own several types of players, even if the players are software-based players. Standardization of a player is the only way content from different DRM providers can be expected to play, and be allowed to play, on one given player. The player is the equivalent of a retail store for a DRM product — if products cannot be attractively displayed, handled and bought within its framework, it's very unlikely that they will be bought at all.

IV Boundaries to Standardization

By this point, it is clear that the reason we want to standardize DRM is to create a viable marketplace for digital content consumption in the face of rampant opportunities for piracy and rapidly decentralizing distribution networks. The viability of a solution demands the following:

1. DRM-protected content from any source within the standard infrastructure should be fairly, normally and easily usable by the user within the standard player. (More about fair use later)
2. “Owners” of the original digital content should be able to govern and enforce the policy of use of the content reliably, economically and fairly.
3. Branding, distribution and service should be an integral part of the system.

Additionally, from a security and privacy point of view, the following salient requirements emerge:

1. The resulting system should be continuously renewable for security breaches, policy and pricing updates and improved cryptography or content management mechanisms.
2. Security breaches should be quickly and accurately determinable.
3. Tracking of individual user behavior may be illegal under local laws. Thus, information needs to be abstracted or aggregated anonymously, not withstanding point 2 above.
4. Exact details of individual companies’ security implementations cannot be expected to be made public. While open inspection is a virtue for specific algorithms and protocols, actual system implementations (especially key management and watermarking) are almost always proprietary and heavily IP-governed. They are the differentiating factor of any DRM provider and therefore necessarily confidential.

For player manufacturers, on the other hand, openness of protocols and incoming format is a definite necessity for design and large-scale production. While more applicable to hardware players, this is nevertheless true for software players as well. Creating multiple players for different design and data-flow considerations is difficult and expensive. Given that software players are almost always distributed for free, unity of design is as much of a virtue for them as for hardware players.

The idea then, is to standardize anything that helps achieve the reasons for which standardization is important, while steering clear of areas that are central to brand and business building but do not affect the universality of the standard infrastructure. This intentionally sounds closely like the MPEG and ITU-T doctrines of standardization. H.26x and MPEG standards have not succeeded by accident. They succeeded because they bridged willingly participating device makers, content owners, users and distributors in a mutually beneficial standard framework.

For each component listed earlier, we now specifically discuss facets that could, should and should not be standardized. We also indicate existing standardization initiatives where appropriate.

IV.1 Identification Mechanism

This should be, and almost always is, completely specified. Several niche standards exist, such as ISBN numbers for published works. Universal digital item identification is rapidly gaining momentum³⁹¹. Part of MPEG-21 also deals with

digital item identification³⁹². Typically quite utilitarian and non-controversial in nature, this is arguably one of the simplest items to standardize. Attention should be paid to the types of content to be supported by the standard, and the specific means of identification that would be useful from purchasing, stock-keeping and searchability points of view. Often, supplementary metadata standards are defined to aid searchability. Two examples of fundamental technology are the Dublin Core³⁹³ and MPEG-7³⁹⁴. These are typically adapted as required into a given standard (such as OpenEBook).

Another set of entities that need to be identified are the DRM and IPMP systems themselves, and the merchants and institutions that they service. Such identification is typically done via fixed-field numbers assigned by a designated registration authority.

IV.2 Secure Transmission and Storage Mechanism

This involves two distinct activities — standardization of a file format and standardization of data obfuscation, or encryption, mechanisms³⁹⁵.

Typically, file formats are standardized within the parent body dealing with a specific type of content. For instance, the MPEG-4 standard specifies the MPEG-4 File Format³⁹⁶, and OpenEBook specifies its presentation format³⁹⁷.

Standardizing on a single encryption mechanism, however, is a recipe for disaster. In today's rapidly evolving computational universe, no algorithm is universally applicable or eternally trustworthy. Additionally, it is impractical from both a standards and commercial perspective for all interested parties to converge on a single algorithm for all possible applications. Nevertheless, the design of a player and intermediate technology often requires an identification of the encryption algorithm being used. This is a simpler problem to solve — a list of acceptable/supported encryption algorithms and modes of use and a means of indicating the same should be part of any DRM Standard. This list should be maintained by an organization so that it can be updated over time as deployed algorithms are broken, new algorithms are developed, and new applications emerge. OPIMA³⁹⁸ and MPEG-4 IPMP Extension³⁹⁹ offer good examples of such a provision.

³⁹¹ See: DOI Standards.

³⁹² See: MPEG-21 Vision, Technology & Strategy (2003).

³⁹³ See: DublinCore.

³⁹⁴ See: MPEG-7 (2001).

³⁹⁵ We will use encryption to mean obfuscation henceforth for simplicity, although encryption is more limited in scope.

³⁹⁶ See: MPEG-4 IPMP Hooks (2001).

³⁹⁷ See: OpenEBook.

³⁹⁸ See: OPIMA.

³⁹⁹ See: MPEG-4 IPMP (2002).

IV.3 An Ownership Tracking Mechanism

For simplicity, we'll refer to all ownership tracking mechanisms as watermarking, despite the loss of scope. The same argument that applied to standardizing a single encryption algorithm works here. The issue more so applies here since watermarking schemes are typically fully proprietary and not open for public review. Enumeration of algorithms is most certainly the way to go. On the other hand, the expected results from watermark detection are usually of specific types, and can be standardized within sufficiently specific markets. Similar considerations apply for fingerprinting and copy marking as well. This allows subsequent processing and infrastructure, such as copy control or radio station play monitoring, to be standardized.

IV.4 Rights Expression Mechanism

XML schemas have widely been accepted as the best means of standardizing a rights expression mechanism. XrML⁴⁰⁰ is by far the most popular starting point for standardization, having been adopted as a starting point by MPEG-21, OpenEBook and OASIS⁴⁰¹. XMCL and ODRL are other rights expression schemas. While under discussion for standardization in niche groups, both have yet to gain widespread acceptance.

A user-initiated action on protected content is an intent. A critical challenge in designing a rights expression standard is to unambiguously define an intent and to clearly define the situation that allows that intent to be fulfilled. As an example of the former, consider the intent to “play”. Play once, play several times, play in entirety, play partially, play backwards or play in fast forward mode are all possible types of play. However, from the DRM point of view, these are significantly different events! Multiple plays will often cost more than one play, and if a user skips an ad while playing back then she might be violating terms of the purchase. This leads us to the latter issue — the situation in which an intent is allowed. If the user paid extra for a commercial-free experience, then skipping the commercial during playback should be permissible and possible. Also, playback might be permitted at full resolution on a high-security playback device, but only at a lower resolution with degraded quality on a low-security device.

Another challenge with rights expression is to ensure that, while clearly specifying the fine details of the rights and payments, the resulting document is significantly small compared to the media itself. Much of the attractiveness of digital media is its accessibility over the net, thanks to high compression. If the license is ten times the size of the file, the solution won't be viable. Many simple compression techniques could be used to mitigate this problem. For more stringent compression areas like MP3 download, however, context-based com-

⁴⁰⁰ The XrML Specification, available at: <http://www.xrml.org>.

⁴⁰¹ See: OASIS.

pression schemes such as those employed by MPEG to compress Binary Format for Scenes (BIFS) streams might be more effective.

IV.5 Authentication Mechanisms

This is a third area where standardizing one single algorithm or scheme is impractical. In terms of certificates themselves, X.509 and derivatives thereof are the most commonly used format. For signatures and key lengths, however, listing a set of algorithms and modes of use is usually a more viable specification. In addition to algorithms, authentication protocols need to be listed as well.

The aim of authentication is to establish that the other entity being communicated to is known and trusted. However, the entire issue of establishing trust is extremely difficult, as the notion of trust itself is hard to define in the technical domain. Trust is not transitive in general, i.e. A trusts B and B trusts C does not *always* imply A trusts C in a DRM scenario. Trust may be manifested in terms of a variety of contracts and obligations, as well as tests. More about trust frameworks later.

In the Internet world, companies such as Verisign act as repositories of a trust in a way, and a holder of Verisign's trust is usually universally trusted though to differing degrees. Similar mechanisms for building webs of trust must be standardized within a specification, as should be an authority or authorities that can extend *and revoke* such trust. DVD is a great example of the consequences of not having revocable certification. Webs of trust can be established in myriad ways — PGP and S/MIME models being two starkly contrasting examples. While the PGP model of individually building trust networks is far safer, the simplicity of S/MIME's transitive trust model makes for a far more usable system.

Typically, recovery from failed authentication and verification is a value-added service available from the player and content provider, and usually does not need to be standardized beyond a minimal graceful failure specification.

In general, the result of successful authentication is a secure communication channel and identification of the end-points. The algorithms and modes for the establishment and use of such a secure channel should either be fully specified or enumerated, depending on the flexibility required by specific instances of a standard implementation.

IV.6 The Secure Player

A complete IPMP System is the synthesis of all the above components along with a playback specification. Within the player, all steps from access of the content to its flow within the player, points of control by different IPMP systems and storage and rendering of the digital item(s) within the player should be completely standardized. The environment in and upon which playback happens also needs to be clearly characterized in terms of security and capability levels. Capability characterization is often an important determining factor for a license.

For instance, one would not want to pay the price of HDTV (1080i) playback on a device with a 352×288 monochrome display.

Also, several IPMP systems will typically work together on content in a secure player. The interaction between them and the order in which they work on the data must be standardized. One of the major weakness of MPEG-IPMP Version 1 was that it provided for a given standard player implementation to work with only one IPMP system. Finally, it is quite likely that certain computationally intensive functions such as decryption will be natively implemented within a player application — it is economically infeasible to include multiple discrete decryption engines as part of each IPMP system. Thus, there needs to be a standard, yet trusted way, for IPMP systems to avail of such services from the secure player. OPIMA made a significant pioneering effort in the design of workable playback platforms. Although OPIMA's design had significant flaws and was never really implemented, it provided useful inspiration for other successful player-side specifications — the most significant being the MPEG-2 and MPEG-4 IPMP Extensions.

Any interface between independent DRM systems or between the player and a DRM system must be fully standardized in terms of calling circumstances, resulting behavior and syntax and semantics of arguments and messages that pass through the interface. Actual implementation of the interfaces is security sensitive. While means of securing that interface may be enumerated with a registration authority, it is quite likely that these will be implemented via proprietary techniques, stacks and stubs.

The current MPEG-IPMP Extensions specification⁴⁰² is perhaps the only standard that fully addresses a secure player. While a full discussion is beyond the scope of this paper, the following are its salient provisions:

1. IPMP Protection is specified in terms of “IPMP Tools” rather than complete “IPMP systems”. An IPMP tool maybe composed of other IPMP tools. The IPMP specification allows multiple IPMP Tools to be configured in a variety of ways to function together as an IPMP system at playback time.
2. In the bit stream, an IPMP Tool List is defined, that is sent before any content and identifies all the IPMP Tools that will be required to process the content. This allows the player to obtain, out of band, any IPMP Tool that it is missing, before the presentation starts streaming. Sets of tools that form equivalent alternatives to each other can also be specified.
3. There are specific commands to indicate the points within the player (called control points) where an IPMP Tool is active. Specified syntax also provides a definitive order of operation of multiple IPMP Tools at a given control point.
4. At the Terminal, a messaging infrastructure is provided that allows all IPMP Tools to be treated, and implemented, as plug and play modules. Tools communicate with other Tools via messages with standard syntax, which abstracts any platform or implementation-specific interface issues.

⁴⁰² See: MPEG-4 IPMP (2002).

5. A Parametric Infrastructure is provided to improve portability of protected content across MPEG-4 Terminal implementations. This provides for:
 - a Selection of an implementation of a Tool, usually available at the Terminal, that implements a specified functionality, rather than answers to a specific Tool Type.
 - b Configuring existing IPMP Tools into new combinations, enabling different types of protection schemes.
6. Specific protocols and algorithms are listed for different types of cryptographic operations including signatures, certificates, authentication, encryption, decryption and watermarking.

V Fair Use

An important requirement for public acceptance of a DRM system is that it allow “fair use” of protected content. Users *expect* some degree of flexibility in use of *their* content, and failure to meet those expectations is commercially fatal. Fair use largely refers to customary usage scenarios of comparable content items that are not protected by DRM today, such as printed books, television programming or CDs. Note, however, that DRM systems can only go so far in enabling such use. DRM systems typically issue licenses to content, as opposed to offering outright sale of a copy⁴⁰³. Hence, the types of use allowed becomes a business and policy issue that is governed by the owner of the IP and possibly negotiable by the end user. Standards can only, and should only, provide a framework to support fair use — they cannot enforce or mandate them one way or another.

The eBook world models their policy along the lines of usage of a traditional book and is a good example of successful fair use enablement. For example, eBooks can be lent or sold by the user, just like traditional books. Digital content in general needs to follow a similar model. The debacle with copy-protected CD’s that won’t play on computers and cars offers a great example of what not to do.

Law in most jurisdictions requires the provision for fair use, although to varying degrees. On the other hand, local and national notions of fair use are difficult to define and enforce in a borderless networked world. Thus, maintaining usage policies based on national laws is a difficult problem and solutions are difficult to sustain given the prevalence of computers and purely digital media. Computers have no nationality, and even network addresses are not national. For example, anyone can own an I/P address block. In fact, class A I/P address blocks are usually owned by multinational companies and hence are impossible to place geographically. The DVD standard does have some region-based rules in place, although these can be circumvented.

Another hurdle to enabling fair use is the sheer difficulty of realizing secure digital alternatives for common use conditions such as lending. A generalized problem of the lending scenario that is popular within the MPEG community (but has yet to be completely solved) is the Gobi Desert problem. Say two people have

⁴⁰³ See: Rosenblatt, Trippe, Mooney (2002).

different player devices, and are in the middle of the Gobi Desert with no hope of any sort of communication to any server. A wants to lend his digital content to B to play on her player. If the object to be lent were a traditional book, this would not be a problem at all⁴⁰⁴. However, if the content is governed by DRM, then several questions arise, such as:

- Given that there is no way to universally block A's rights while he has lent content to B, since there is no network connection, how would the temporary lend be enforced?
- The content does need to be transferred from device A to device B. What sort of watermarking, fingerprinting or obfuscation is necessary to do so in a traceable and secure manner?
- The DRM system allows playback on A's player. But would it allow playback of the same content on B's player? Is the latter trusted?

The issues of transferability of content and trust in general are sticky ones, and the answers are by no means simple. However, perfect answers don't need to exist yet to develop workable standards. As technology and experience evolves, better solutions will be created. Basic trust issues, on the other hand, are a pressing problem to solve. We discuss these briefly in the context of the MPEG IPMP Extension work in the next section.

VI Trust Framework

Three requirements on the MPEG IPMP extensions have direct impact on the design of security and trust infrastructure for the IPMP extensions: content transferability, device mobility and content mobility. In conjunction, these 3 requirements pose some difficult standardization questions. Namely, these requirements resolve down to the difficult question of how two devices, which are disconnected from any external networks, can achieve the following:

1. Determine whether to trust each other in a standardized fashion
2. Determine the legitimacy of a transfer request in a standardized fashion without access to an authoritative third party
3. Effect the transfer of the content in a secure and standardized fashion

Determining the legitimacy of a transfer request can be accomplished using a standardized RDD/REL-based query on the usage policy associated with the content in question after the establishment of a trust relationship between the devices. Securing the content transfer can also be done using well-known cryptographic means. The question of trust quantification, however, is a hard one, as the nature of trust relationships spans commercial, contractual, societal and technical domains. Since much of trust lies outside the technical domain, the challenge from the standardization perspective is to *permit* the expression of

⁴⁰⁴ Several wise people have argued that even with digital content, this is not a problem — A and B can simply swap players, or B can listen while A plays the music. However, that is not exactly the sort of solution that was and is being sought — the music needs to be playable on B's player.

a trust relationship and design the framework to codify this expression. The process and procedure for the establishment of a trust relationship is outside the scope of standardization though it is useful to note that a web of N -party bi-lateral trust relationships will not scale gracefully.

The most realistic way of describing trust levels is via one or several metrics that quantify, so to speak, the amount of trust required for a certain scenario. The basic driver behind digital rights management is the protection of content. The value of this content seems to be a natural metric to use for trust — after all, the higher the content value, the more the security and hence the higher the level of required trust. However, content value is usually unsuitable as a single quantifier of trust requirements as no systems, DRM or otherwise, can provide absolute levels of protections against all attackers for an indefinite period of time regardless of the value of the content. Furthermore, content value, while useful, is not consistently quantifiable as some content may have little extrinsic value but great intrinsic value. Therefore content value is not useful in specifying the trust metrics.

The trust requirements for any DRM system have to be considered principally in 3 dimensions: level of protection offered, duration the protection required and the time frame. Useful trust metrics should combine these three characteristics in a manner suited to the applications that the standardization effort will target.

To avoid the scaling issues associated with N -party bilateral relationships where $N!$ relationships are required, we have to look at codifying indirect trust relationships. There are many indirect trust relations that occur in everyday life. Take the example of the national passports. A passport is a time-limited trust bearing instrument that is granted to a citizen by one's government. When one presents the passport at a border, passport control will firstly check the validity of the passport and then check the person carrying the passport before the person is permitted to enter the country. Through trans-border agreements and standardized passport technology, the legitimate bearer is permitted to enter the country even though the bearer and the pass control officer never establish a direct trust relationship.

The IPMP standardized trust framework manages the trust metadata associated with the IPMP tool/terminal. The trust metadata is similar to a passport in that it is a time-limited trust bearing instrument that is presented by one DRM component to another. The trust metadata is pre-authenticated and possibly digitally signed by a trusted third party. It will have a standard structure and contain pre-agreed upon information. And lastly, it has an explicit expiration date that is necessary for all trust bearing instruments. Passports can be copied given the proper motivation and resources. Trusted DRM components can similarly be cracked given enough time and the right tools by those with the right skills.

VII The Tradeoffs, and Lessons from the Past

As in any design problem, there are some salient trade-offs that need to be considered while standardizing a DRM framework.

Chief among them is the need to standardize interoperability-sensitive areas while keeping security-sensitive components confidential. Open interfaces and algorithms allow for strong peer review as well as interoperable implementations. However, trade secret and insurance issues, brand differentiation and differing technical and legal opinions often make open standardization impracticable, as SDMI demonstrated.

Middle ground can typically be achieved using a combination of enumerated algorithms, controlled-access algorithm definitions and proprietary control and service streams. The Conditional Access system used for DVB is a brilliant example of a perfect balance. Flexibility of encryption is allowed using Simulcrypt and Multicrypt schemes, while the actual transmission and playback format (including key rotations) is fully standardized. Actual key delivery streams and payments are handled by each CA company on a proprietary basis. The encryption algorithms are stored in the custody of ETSI and available to interested parties upon certification. Continuous renewability of the receiver ensures that hacks can be dealt with in a timely and efficient manner. The DVD standard, on the other hand, chose to use a less restrictive specification that allowed self-certification and was quickly broken. Notwithstanding the breakage, however, the DVD is a hugely popular and commercially successful format. Almost all new titles are released into the format and DVD players are widely available at lower and lower cost. In our opinion, that makes the DVD specification a success. At the far end of the spectrum is the completely open SSL specification. Extensive and continuous peer review ensures, at least on paper, the security⁴⁰⁵ of communications secured by SSL. On the other hand, knowledge of the algorithm places tremendous responsibility on any implementation to be bug-free. Any weakness, typically in the random number generator, can be rapidly exploited to create a hack.

The second major trade-off while creating a DRM framework is that of security and complexity v/s acceptable loss from piracy. A given standard needs to carefully evaluate the value of content that it will service, and the corresponding realistic security requirements that it needs to meet. The higher the bar of a DRM framework, the more expensive it is to create and maintain, and usually the harder it is to use. Extremely stringent security requirements and provisions are in order for standards such as Digital Cinema, where full resolution movie prints for theatres are being transmitted and monitored. Given the higher stakes of a potential breach, the higher costs of implementation are fully justified. For DVD, on the other hand, the loose security system works just fine. Algorithms

⁴⁰⁵ All cryptographic systems have a finite half-life. Potential algorithmic weaknesses discovered through analysis and fixed key sizes limit the useful life of a cryptographic system.

and methods offering higher security could have resulted in \$2000 players and \$100 DVDs — unacceptably high costs for the target market.

The third consideration is the level of flexibility to be enabled. Enabling every application from buying a single newspaper copy to super-distributing⁴⁰⁶ 55 variations of a specific song according to regionally differing laws is wonderful, but could make for a completely unimplementable standard. A very strong focus on the application sphere is essential, even though it may be hard to maintain given the sheer variety of application possibilities, especially in a software world. Another form of flexibility that demands attention is the design and implementation of DRM systems for the standard. The MPEG-4 Version 1 IPMP (commonly called the “Hooks”) Specification is a great example of a well-intentioned effort that erred on the side of too little specification for the IPMP System, resulting in an undesirable environment where only one compliant IPMP system could be guaranteed to work per compliant Player implementation. The extensions have come much further in reducing the ambiguity of specification, creating a more viable standard where standard IPMP Tools and extremely likely to work with standard Players, assuming appropriate trust relationships exist.

The final, and most important, tradeoff is that between the interests of the player makers and the IP owners. Player makers serve the end user — they need mass-market appeal to succeed and thrive. However, they also need content to play on the players in order to create a market in the first place. On the other hand, content owners need the player to protect their own interests of minimizing content theft while allowing fair use of the content at the same time. The balance between the two is difficult to achieve — indeed, Sony often finds itself on two opposing sides of the table, owing to its player and label interests. Yet, a standard that alienates either one of the parties is doomed to obscurity. OpenEBook is an example of a standard that deals well with this problem — publishers, software providers and device makers are all active, and mostly harmonious, participants. SDMI, on the other hand, is a good example of the stalemate that can result when developing standards that alienate device makers.

VIII Implementation Technologies

Even though implementation technologies are outside the scope of standardization, it is worthwhile to present a short summary to set the technology landscape. Available technologies have direct impact on feasibility and very few useful standards are defined without consideration of feasibility. In fact, an explicit requirement of the MPEG IPMP Extension effort was that standard proposals be based on available technologies.

Ultimately, a standard only specifies a framework. Implementations of a standard are achieved by use of secure technologies such as secure platforms, inter-module communications, cross-network communications, storage, key retrieval and computing.

⁴⁰⁶ Superdistribution refers to the ability for intermediaries to redistribute content.

Technologies for securing communication between modules are well understood though not always properly implemented. Cryptographic technologies, whether based on symmetric or asymmetric ciphers, are commercially available technologies that could easily secure the communication between modules.

Issues with any large scale cryptographic deployments are almost always related to key management. The traditional means to deal with cryptographic key distribution is either to embed the key in tamper-resistant and tamper-evident hardware such as smartcards, dongles or cryptographic processors, or to embed the key in consumer electronics as DVD players do with CSS keys. This serves to convert the abstract problem of key management to the real one of managing a piece of hardware. Due to the cost of reverse engineering hardware to extract cryptographic keys, this also serves as fairly effective protection against key recovery against casual attackers.

The economics and technology of S/W-based players are quite different from those based in H/W. The incremental manufacturing cost of S/W players is negligible and so is the cost of reverse engineering the player. The hardest problems that must be dealt with by all S/W-based DRM system implementers are to prevent an attacker from modifying the S/W or stealing the cryptographic keys.

We describe possible attacks before discussing protective solutions. There are plenty of commonly available tools like decompilers, optimizing compilers, disassemblers, and debuggers that allow an attacker to modify software or extract cryptographic keys hidden in software. CSS was cracked using some of these simpler tools and techniques applied to a S/W-based DVD player. A debugger-based attack can be extremely effective in the knowledgeable hand.

More advanced attacks like fault injections, virtual machines or in circuit emulators are currently not readily available to or usable by the average amateur attacker but are available to well funded attackers. These more advanced attacks will be more readily available in the future as technology progress reduces the cost of the equipment necessary to mount one of these attacks.

Two classes of tamper-resistant software technologies are being used to realistically protect DRM systems from amateur attacks. One class involves applying cryptographic techniques to the software and any related secret until the very last instant before execution. Aucsmith⁴⁰⁷ has proposed using a rolling XOR mask for that purpose. The issue for this class of technology is the generation and storage of the cryptographic key or the initial XOR mask needed to decrypt and execute the software.

The other class of S/W tamper-resistant technology is software obfuscation. Various academic research efforts⁴⁰⁸ exist in this area. Various commercial implementations of this technology, of differing strengths of protection, are known

⁴⁰⁷ See: Aucsmith (1996).

⁴⁰⁸ See: Collberg, Thomborson (2002); Wang (2000); Devanbu, Stubblebine (2000); Appel, Felten (1999); Collberg, Thomborson, Low (1997/1998).

to be available at the time of writing. Software obfuscation basically applies various tamper-resistant transformations to normal software to turn it into tamper-resistant form of S/W. Depending on the transformations applied, it may be possible to actually hide cryptographic keys in the transformed S/W.

It is worthwhile noting that all effective tamper-resistant technologies will have a significant time/space penalty. They cannot, in general, be applied to complete systems, as the overhead is too high. The unavoidable transition between the tamper-resistant form and ordinary form of S/W will always be the easiest point for attack and needs to be designed very carefully. For effective results, the use of tamper-resistant technologies needs to be incorporated into the design of the DRM system upfront rather than be applied as a post-development patch.

IX Current Standardization Activities

By far, the most exciting standardization activity related to IPMP systems is within MPEG — via its IPMP Extension work for MPEG-2⁴⁰⁹ and MPEG-4⁴¹⁰, and various activities in MPEG-21. At the time of writing this paper, MPEG-4 IPMP extensions specification is an international standard, and the MPEG-2 extensions are almost finalized. MPEG-21 is still under development — while the Digital Item Declaration and Rights Expression Language specifications are well defined, other activities such as Digital Item Processing are just getting underway.

OpenEBook⁴¹¹ is progressing, but still has some way to go. The file format is reasonably well specified, as is metadata. Rights and rules will be based on XrML, but the exact specification is just beginning to take shape. The systems layer is yet to be specified, as is any trust infrastructure. The European standardization body CEN/ISSS has just embarked upon DRM standardization⁴¹², and it will be interesting to see if they go beyond a simple rights language standardization. The Open Mobile Alliance (OMA) recently released version 1.0 of its DRM standard for mobile devices⁴¹³. This provides an end-to-end specification for clearly scoped specific usage scenarios within mobile devices. Meant for low-value content, it has no authentication and limited security features.

⁴⁰⁹ See: MPEG-2 IPMP (2002).

⁴¹⁰ See: MPEG-4 IPMP (2002).

⁴¹¹ The OpenEBook Specification homepage: www.openebook.org.

⁴¹² The CEN/ISSS DRM homepage: <http://www.cenorm.be/iss/DRM/Default.html>.

⁴¹³ See: OMA.

X Conclusions and Summary

As the progress or demise of past standardization attempts shows, certain aspects are vital to the creation and deployment of a successful DRM standard. These include —

- Clearly defined goals and applications,
- Clear evaluation of value of content and corresponding level of security requirements,
- Benefits to both player manufacturers and content owners, and
- A good balance between enforced interoperability and room for entrepreneurship and branding.

Additionally, support for “fair use” is a critically important factor for a DRM framework in order to enable commercially viable applications.

No DRM standard can consist only of bound sheets of paper. A living, updateable and flexible technical infrastructure and a human organization to maintain ongoing security issues must support it. Institutions are required for safekeeping of sensitive material, for initial and on-going certification and for facilities for security inspection and auditing where applicable.

DRM is essential to realize the power of digital distribution of multimedia. Ease of use is paramount for successful DRM-based systems. An important requirement for ease of use is the feasibility of a generic player and server for use of protected content from multiple sources. Standards are the only way to enable this, and hence are essential to widespread acceptance. DRM standards that require every bit and byte to be set in stone are difficult to create and impossible to enforce and implement. Luckily that’s not necessary — successful examples of a middle ground exist.

A standard can only build a framework; it can’t plug all the leaks. That has to be done by use of such technology such as secure platforms, inter-module communications, cross-network communications, storage, key retrieval, computing.

Finally, it must be realized that protection offered by DRM systems is not and will never be absolute. DRM systems must be thought of as a rearguard. Any DRM system can be defeated; even the most paranoid one. One favorite story of mine is from a colleague who was asked to check the breakability of a truly sophisticated audio protection system. He simply legitimately played the music, recorded it to tape via a microphone, digitized and recorded it, and pronounced it broken. Acceptable though imperfect DRM systems can and should exist in the meanwhile. As long as it enables the market it is supposed to, and keeps revenue or information losses within acceptable levels, it is successful. The credit card business is an apt parallel of a fallible system that still makes for a very lucrative business. Understanding this, clearly specifying the requirements for protection up front and understanding limitations is crucial to the success of any DRM standardization and deployment.

2.6 Trusted Platforms, DRM, and Beyond

*Dirk Kuhlmann*⁴¹⁴, *Robert A. Gehring*⁴¹⁵

I Introduction

It is not immediately obvious why a book on Digital Rights Management should include a chapter about Trusted Computing, although a number of publications have investigated the suitability of trusted systems as rights management platform. Until recently, however, they have been of little more than remote interest for DRM as well as for typical business or consumer environments, as they were considered to be inflexible and cumbersome to manage.

This has changed dramatically with the advent of the technology developed by the Trusted Computing Platform Alliance (TCPA). Although this technology has primarily been propagated as security improvement of networked end systems, multiple observers were quick to point out that some basic features were similar to mechanisms that allow to support DRM. In some extreme cases, TCPA has literally been equated with DRM, this is, as a thinly veiled attempt to introduce ubiquitous control mechanisms on formerly open PC architectures.

As an introductory remark, it is sufficient to point out that the apparent contradiction between “openness” and “full user control” on the one hand and “closedness” or “constrained user behaviour” constitutes a similarity between requirements of DRM and system security. Consider computers in organisational and corporate environments: once a machine is part of a collaborative network and processes data that is subjected to external policies, full user control gives rise to a number of problems. It allows users to install and run arbitrary software for both corporate and private purposes. This can easily create security vulnerabilities, something network administrators are very aware of keen to prevent.

Copyright holders are facing a similar problem. Personal computers can include software media players to display digital content, but as the user has full control, they can also be used for storing, duplicating, and disseminating the content in ways not endorsed by copyright regulations. The proliferation of cheap and powerful multimedia PCs and the convergence of digital storing technology (e.g., compact disc) has created a situation where copyright owners have effectively lost control over digital copies of their works.

These and other dilemmas have renewed the interest in mandatory control mechanisms and trusted systems. These systems can enforce rules users have to adhere to when interacting with resources that have multiple stakeholders. In other words: the user can not override the policy while maintaining access to the resource subjected to this policy. This can significantly improve confidence in the expected behaviour of an IT system as it allows fine-grained control over what

⁴¹⁴ Hewlett Packard Laboratories, Bristol.

⁴¹⁵ Technische Universität Berlin.

computers and their users can do at any given time. TCPA and Trusted Platform technology claim to address the problem of how to gather and communicate indicators about what behaviour to expect.

This paper is an attempt to scrutinise arguments that concern TCPA's potential as DRM technology. We will start with an outline of TCPA (v. 1.1b) in terms of its context, basic features, and critique it has encountered, followed by an overview of trusted systems in general that discusses both the traditional concept of 'trust' in IT security and more recent attempts to apply this approach to digital rights management. This allows us to analyze commonalities and differences between traditional and DRM-focused trusted systems. We conclude with a discussion of the future of Trusted Platform technology and some thoughts on technology regulation.

II Trusted Computing Platforms

IT security vulnerabilities have become an increasing problem during the recent years. As of 2003, an average of 11 new bugs are reported every day⁴¹⁶, and this number is rising. As a consequence, security remains a major concern for both corporate and private IT users.

There are a number of factors that contribute to this situation. To name only three of them:

- Most users have little if any idea about what is going on behind their graphical user interface. Even administrators frequently do not have a comprehensive understanding about what is actually happening on their machines.
- All software can be tampered with before or while it is running. As a consequence, systems whose security relies on software alone ultimately can not vouch for their own status and integrity.
- Even if our current IT systems were more secure, they could not communicate this fact in a trustworthy manner to remote peers. Trust relationships between technical systems currently have to be established out of band by their owners.

The current lack of confidence the security of IT can at least partially be attributed to two major advantages of today's end systems and networks — namely, their openness and flexibility, which are often considered as fundamental values. However, one might argue that the extent to which a system should be flexible and open depends finds its natural limitations in the purpose it serves to its owner and his communicating peers at any given point in time. In some situations, maximum openness and flexibility are desirable. In others, the exact opposite might be true.

Systems that put emphasis on security rather than on versatility have traditionally been designed for environments where concerns of confidentiality, integrity and separation of roles are prevalent under almost all conditions, e.g. for the

⁴¹⁶ See: CERT (2003).

military and financial sector. They tend to be governed by rigid polices, and much research has been done to find suitable access control mechanisms, in particular for operating systems⁴¹⁷. Unfortunately, these designs tend to counteract the aforementioned advantages of openness and flexibility while simultaneously imposing a penalty of additional system management.

Trusted platform technology as discussed in the following sections claims to combine the advantages of both worlds. It starts from the understanding that in everyday situations, security is a flexible notion rather than an absolute goal: in order to be trustworthy, a system just has to be secure enough to be fit for purpose. Trusted platforms do not insist on provable security for all conditions – even less so since the user may not understand and therefore not trust the proof. It is deemed more important that a trusted party vouches for the fact that a particular system configuration and policy is fit for a particular purpose.

Apart from enforcing policies, Trusted Platforms address two other problems mentioned above. The design sets out to provide for a mechanism to reliably record the system state and to report it upon request. This allows to communicate state information from a local machine in a way that is trustworthy to a remote party.

II.1 The Trusted Computing Platform Alliance

The Trusted Platform Computing Alliance (TCPA) was created in 1999 by Compaq, HP, IBM, Intel, and Microsoft, all of which became members of the organization's steering committee. Since its creation, the TCPA has been joined by more than 170 other companies and organisations. Apart from the major platform and software companies just mentioned, the consortium includes, amongst others, chip and BIOS producers, vendors of authentication or security technology and services, and financial or content service providers.⁴¹⁸

Although the alliance started out with a PC specific agenda, TCPA design characteristics now cater for other a wide range of networked IT such as servers, network appliances, mobile phones, PDAs, and consumer electronics. This has broadened TCPA's appeal even further, and while this article is written (March 2003), the consortium is undergoing a major process of reorganisation that accommodates a wider and more diverse membership.

Since its formation, the alliance has created the current TCPA "Main Specification" 1.1b⁴¹⁹ and a PC-oriented "Implementation Specification"⁴²⁰. For the TCPA hardware component, the "Trusted Platform Module" (TPM), was defined, and its version 1.9.7⁴²¹ has since been certified by NIST according to the Common Criteria Evaluation Assurance Level EAL3+⁴²².

⁴¹⁷ Overviews can be found, e.g., in Pfleeger (1996); Anderson (2001); Bishop (2003).

⁴¹⁸ For details, see the TCPA membership list at:
<http://www.trustedcomputing.org/tcpaasp4/members.asp>.

⁴¹⁹ See: TCPA-Spec (2002).

⁴²⁰ See: TCPA-SpecImpl (2002).

⁴²¹ See: TCPA-TPMProf (2002).

II.2 TCPA — Motivation and Approach

The IT industry sees itself under increasing pressure from government, businesses and consumers to improve security aspects their products and services. So far, the success of respective efforts has been quite limited. This can partially be explained by the fact that neither the Internet protocols nor the PC have originally been engineered for the purposes they are used for today.

The common Internet Protocol (IP) ignored security aspects almost completely. The same is true for many transport, signalling, and management protocols that constitute the building blocks of today's infrastructure and have been built on top of IP. As a consequence, deployment of security enhanced systems becomes difficult as soon as contributing nodes are part of different organisational domains and subjected to different policies. This situation is increasingly typical for today's Internet: current practices of outsourcing, contracting and collaborative work make it desirable to allow access to precisely defined subsets of system resources, and there is an increasing need to support policies even across organisational and corporate levels.

PCs and their operating systems were originally designed for standalone purposes. Over the last two decades, they have been continuously extended to make them usable as network nodes. Workstations and other end systems now include features that would previously have been considered as elements of networked servers. This has made them more vulnerable to remote subversion and more suitable as tools or launching platforms for hostile attacks. This problem of end point security and trustworthiness is the one TCPA has set out to address.

Given that it was possible to create such a broad industry alliance to tackle end point security, one can safely assume the existence of major technical, economical and political drivers behind the agenda of trustworthy computing. Existing technical deficiencies and continued governmental pressure are likely to play an important role here. Apart from this, there are straightforward economic factors that may motivate support of TCPA's agenda. Depending on their respective commercial activities, consortium members could be motivated by the following considerations:

- TCPA requires an additional hardware component to be embedded on motherboards, which makes this technology interesting for chip producers.
- TCPA relies on security validation and certification, which makes it attractive for evaluation laboratories and PKI vendors.
- Lack of adequate security for end systems has been named as a major inhibitor for ubiquitous e-business and e-government, and e-service providers may see TCPA as enabling technology.
- Last, but not least, content providers and software vendors are likely to view TCPA as a promising technology to protect their rights on digital content⁴²³.

⁴²² See: NIST (2002).

⁴²³ Content protection is not copyright protection since the copyright laws do not acknowledge mere "material" and/or "metadata" as subject matter for copyright protection. The paradigmatic change hidden behind this chosen terminology ("content") is broadly discussed in: Bechtold (2002).

Given the extent of TCPA's intended usage, security requirements will vary widely due to different usage contexts and platforms. To comprehensively cover this variety in a technical specification is close to impossible, which is likely to be the reason why TCPA steers makes minimal assumptions about usage scenarios. It assumes little more than that every platform has an owner. In addition, the specification reflects the common situation where users do not own the platforms they are working with.

One of TCPA's most emphasised features is a set of mechanisms to reliably record and report the configuration and state of a platform. Since trustworthiness is a multilateral problem in the networked world, reliable reporting not only has to satisfy the local user of a machine, but also peers he is communicating with. Trusted platform technology provides a number of building blocks to address this problem.

There are two ways how users can convince themselves that a system is adequate for an intended action. They either base their decision on their own understanding of technology or they trust a third party that vouches for the system's "fitness for purpose". It should be emphasised that "fit for purpose" is a pragmatic notion and different from "secure". Trusted platforms can support judgements about the level of risk that they might not behave as expected. Secure systems are designed with the goal to minimise or exclude risk. Clearly, secure systems can be built on top of Trusted Platform technology.

Systems that are built on top of TCPA technology can exploit its features to ensure the integrity of the system configuration once it has been accepted. This includes enforcement of any particular policy that is part of this configuration. How they do this is not defined by TCPA; Trusted Platforms technology as such is oblivious to any specific policy or configuration.

II.3 TCPA Technology and Infrastructure

The TCPA architecture consists of three principal elements: hardware, software, and infrastructure (see figure 1).

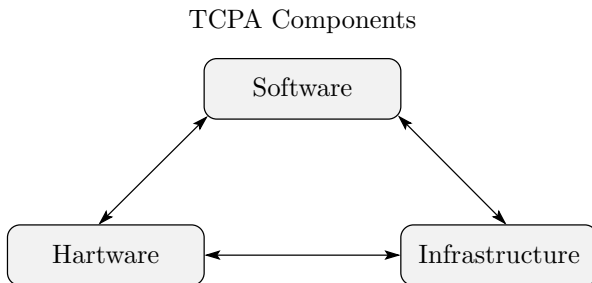


Fig. 1. TCPA Components⁴²⁴

The interaction between these components is quite complex and can only be outlined in this section. For a more comprehensive overview, the reader is referred to

⁴²⁴ Unless stated otherwise, all figures are © 2003 Robert A. Gehring.

Pearson⁴²⁵ and the specification proper⁴²⁶. A number of common misconceptions are addressed by TCPA⁴²⁷ and Safford⁴²⁸, and this article, respectively.

Hardware

The hardware component (Trusted Platform Module or TPM) provides functionality that is roughly equivalent to that of a state of the art smartcard. It includes a random number generator, a generator for RSA key pairs, and a limited amount of non-volatile storage. The non-volatile memory on the chip is considered shielded: at the level of the chip's tamper-resistance, it is protected from interference and prying.

Some of the non-volatile memory on the TPM is used to store two 2048 bit asymmetric key pairs. One of these key pairs, the Endorsement key, is generated at the vendor's premises during production time and is the single unique identifier for the chip. The second pair, the Storage Root Key, is generated when a customer takes ownership of the TPM.

During the process of taking ownership, the prospective owner defines an authorization secret that he has to provide to the TPM from then on to enable it. The private parts of both the Endorsement and the Storage Root keys are stored exclusively inside the TPM. The owner can not use the private part of endorsement key to sign or encrypt data. In order to decrypt data that has been encoded using the public part of the endorsement key, knowledge of the authorization secret is required.

The remainder of the non-volatile memory on the TPM is organised as two sets of registers. A Platform Configuration Register (PCR) is designed to store values that represent the complete history of its modifications; a Data Integrity Register (DIR) has the same size as a PCR. It can hold an arbitrary value of up to 160 bit length that typically reflects the expected value of a corresponding PCR.

Most TPM commands are essentially combinations of the basic functions mentioned above: authorization secret, key protection, key generation, shielded configuration registers and integrity registers. Amongst others, the TPM supports to:

- employing asymmetric key pairs that can not be used by software, but only by a TPM,
- logging system events in a non-reversible manner, supporting reliable auditing of the system's bootup and configuration,
- binding the capability to decrypt data to a specific platform state

Most operations are not provided by the TPM on its own, but need operating system and application software support.

⁴²⁵ See: Pearson, Balacheff, Chen, Plaquin, Proudler (2003).

⁴²⁶ See: TCPA-Spec (2002).

⁴²⁷ See: TCPA-QA (2002).

⁴²⁸ See: Safford (2002a).

Software Support

TCPA compliant end user systems require two types of software. The first type, the Trusted platform Support Service (TSS), implements a number of complex functions that need multiple invocations of the TPM and symmetric encryption functionality. The second type, called “Core Root of Trust for Measurement” (CRTM), is part of the platform firmware. It will typically reside in a BIOS or chipset and executed at an early stage of the platform bootup. Its task is to generate hash values of all binary code that is about to be executed and to log these values into the PCRs of the Trusted Platform Modules.

The core idea is to extend this type of “software measurement” from the firmware and the BIOS to the operating system (OS), OS services and applications. TCPA defines the chain of integrity verification up to the OS boot loader. Specific boot loaders or operating systems are not covered by the specification. As of the current specification, TCPA is OS-neutral.

Infrastructure

TCPA based systems include indicators that help to determine the level of confidence users can have in a given software environment. This judgement can be based on trusted statements of other parties. In order to communicate these statements, TCPA needs support of digital signatures, certificates, and public key infrastructures.

The first certificate concerns the unique identifier inside the TPM, the endorsement key. It attests that the private endorsement key resides on a TPM of a specific type, on this TPM alone and that it has never been disclosed to anyone.

The second certificate attests that a specific TPM with a specific endorsement key has been properly integrated on a motherboard of a specific type.

Platform credentials include a reference to a third kind of credential, the conformance certificate. It vouches for the fact that the combination of a TPM and a specified type of motherboard meet the TCPA specification, e.g., because both meet the Protection Profiles mentioned in section II: *The Trusted Computing Platform Alliance* on page 180.

The last certificate type can combine all aforementioned credentials in a single statement. The TCPA specifications envisages these “identity certificates” to be issued as identifiers for Trusted Platforms. It is noteworthy that:

- identity certificates do not need to reflect attributes of human users in any way, as they identify platforms;
- a single Trusted Platform can have an arbitrary number of identity certificates, hence multiple identities;
- requests for identity certificates do not require to prove platform ownership to a remote party.

Figure 2 shows the composition of TCPA components and their infrastructural dependence on Certification Authorities⁴²⁹.

⁴²⁹ See: TCPA-TPMProf (2002); Pearson et al. (2003).

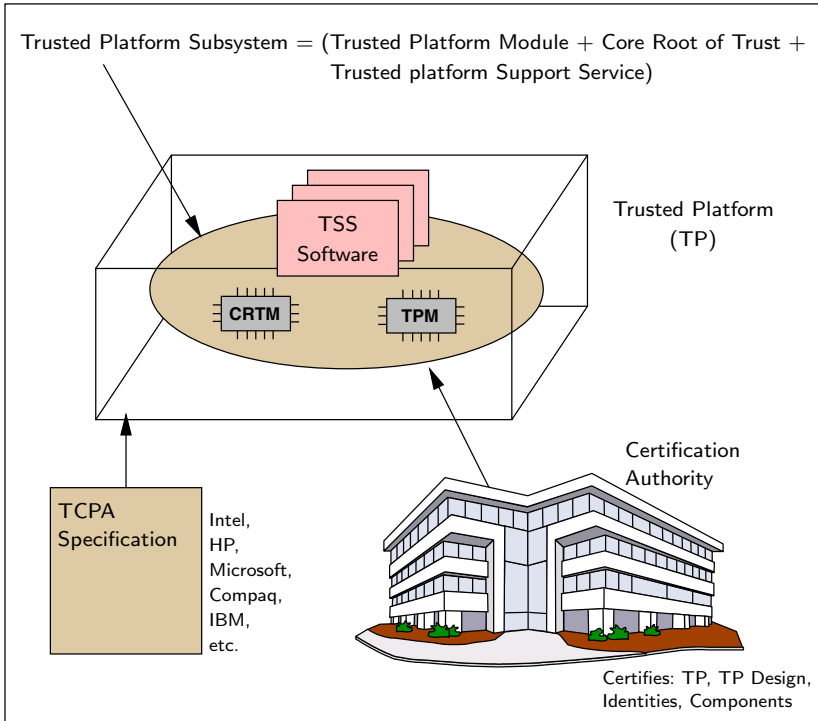


Fig. 2. Composition of TPCA Components⁴³⁰

Certification Authorities (CAs) that issue TPCA identity certificates may follow arbitrary policies since the specification is agnostic about particular CA policies and platform configurations. CAs may require a specific protection level attested as by the conformance certificate.

In principle, all TPCA mechanisms can be used without involving *external* certificate authorities. Platform owners, be it organisations or individuals, can issue identity certificates for themselves.

II.4 Critical Reactions

The concept of “Trusted Computing Platforms” as proposed by TPCA has drawn heavy criticism from security experts, computer scientists and consumer protection organisations even before its deployment.

An impartial observer will, at least in part, blame the TPCA itself for the criticism: The development process of the TPCA specification was not open to contributions or comments from the public and statements of some TPCA members regarding their intentions to deploy the technology raised suspicion of hidden actions and intentions.

⁴³⁰ Source: Pearson et al. (2003): 7.

This section gives a cursory overview of the main arguments of the critique. They can not all be scrutinised for their merits here. However, the most common point, namely, the equation of TCPA with DRM, deserves an in-depth exploration. This will be done in section III of this paper.

The objections⁴³¹ against TCPA can be roughly categorised as follows:

TCPA Means DRM

A number of critics maintain that the main purpose of TCPA is to embed hardware support for Digital Rights and Software management on end user platforms. They question the motives and intentions of the TCPA consortium and, in particular, the large corporations that constitute the steering committee, on principal grounds.

TCPA Means Less Freedom

Critics have pointed out the potential for misusing TCPA technology, e.g. for censorship and customer lock-in. The warnings that TCPA could put restraints on free speech are derived from the same warnings directed against DRM technology.

From a consumer protection point of view, it is claimed that TCPA solves the providers' rather than the users' problem. By supporting to constrain what users can or cannot do with their computers, more consumer value could be destroyed than is created by better trustworthiness.

TCPA Means Less Privacy

Since TCPA is widely equated with DRM, reproaches for undermining privacy directed against DRM technologies are regularly applied to TCPA too. The most important reproach refers to the impossibility of consuming media content in privacy due to the built-in feature of many available DRM systems to collect media usage information and to transfer it to content owners.

TCPA Means Less Security

It has been claimed that TCPA based technology could make reverse-engineering of DRM and security components harder. In conjunction with legal prosecution of reverse-engineering, this may lead to a situation of less rather than more trustworthiness.

TCPA Means Less Competition

Concerns have been raised with respect to potential negative consequences of TCPA in economical, social or political terms. Without objecting to TCPA as such, these critics argue that this technology will inherently cement current quasi-monopolies in the hardware and software sector and may create new ones in the content industry.

⁴³¹ More detailed criticism can be found, e.g., in: Anderson (2003); Arbaugh (2002); Green (2002); Cryptography (2002); Cypherpunks (2002) (from June 22, 2002 onwards).

TCPA Means More Security-Relevant Problems

A number of issues have been named that are linked to TCPA's hardware- and infrastructure based approach. They concern e.g. problems of (a) proving the trustworthiness of the on-chip random number and RSA key generators; (b) consequences for virtualisation layers and emulators; (c) potential large-scale abuse of the mechanism by bogus endorsement and identity certificates dissemination or revocation.

Summary

To wrap up: TCPA critics object the technology on the grounds that Trusted Platforms mean DRM, less competition,⁴³² less freedom — including less freedom of choice, and less control⁴³³ Supporters of TCPA have upheld that much of the critique is based on speculation and limited understanding of the technology, and that mutual assurance for IT systems is a real and pressing issue that is independent of any given political and economic context and has to be addressed where it crops up: at the level of technology.⁴³⁴

A cautionary observer may conclude that both critique and rebuttals are dissatisfying and that further discussion is in place.

III Trusted Systems vs. DRM Systems — Deblurring the Lines

That TCPA should be considered as some kind of DRM is a key part of almost every critical statement about the concept.⁴³⁵ The reasons for this assumption can be traced back to different motives, some obscure ones and some meritorious ones. We find technical arguments mangled with conspiracy theories and ample speculation based on misunderstandings. To make a serious judgement on these issues, we first have to deblur the lines between the concepts of trusted systems, trusted computing platforms, and DRM systems. We focus here on trusted systems and trusted computing platforms because DRM systems are exhaustively treated in this book.

For reasons of historical developments, we start with a portrayal of trusted systems.

⁴³² Most recently Anderson (2003a).

⁴³³ According to prominent critic Ross Anderson, they are probably even less secure, because a “trusted system or component” is defined as “one which can break the security policy”, implying that a “trusted computer” is one “that can break my security” Following this line of logic, the only computer where our security can not be broken is an untrusted one (since no one would expect security in first place). See: Anderson (2003): par. 24, 25.

⁴³⁴ More detailed answers to the critics can be found, e.g., in: TCPA-QA (2002); Safford (2002a).

⁴³⁵ See, e.g.: Anderson (2003); Yodaiken (2002); Weber (2003); Grassmuck (2002).

III.1 The Classic Approach to Trusted Systems

Trusted systems are neither new nor invented by the TCPA. Actually, research on trusted systems dates back to the 1960s and was driven by government and military needs for effective protection of information. The development of the Trusted Computer System Evaluation Criteria (TCSEC) from 1983 to 1999, also known as the Orange Book, was the first culmination of those research activities. Since its development was driven by governmental institutions, confidentiality is the main focus of the TCSEC. Data integrity and system availability, usually goals of information security,⁴³⁶ are of less importance within the TCSEC framework⁴³⁷.

Two research approaches were particularly influential on the formulation of the classic concept of trusted systems:

- The reference monitor concept introduced in 1973 by James Anderson;⁴³⁸ and
- The Bell-LaPadula (BLP) model as introduced in the same year by D. Elliott Bell and Leonard J. LaPadula.⁴³⁹

BLP was developed for a military environment, Anderson's reference monitor has been conceived as a proposal for governmental establishments. BLP is a *policy model*, describing a specific way of controlling access to system resources. It is primarily concerned with restricting the information flow between formally distinguished security levels and compartments. The reference monitor concept, on the other hand, models a *system architecture* suitable to enforce policies. The monitor can be regarded as container to be filled with a rule set of choice (which could follow the BLP model as well as completely different ones). This concept is more generic, as it allows to employ arbitrary policies that might be better suited to meet modern business requirements for sharing information than the rather restrictive BLP.

The following short discussion may help to understand some peculiarities of the TCPA approach to evolve ordinary computers into trusted computing platforms. We start with pointing out some basics of the reference monitor concept.

The Reference Monitor Concept

According to Bishop⁴⁴⁰, “a reference monitor is an access control concept of an abstract machine that mediates all accesses to objects by subjects.” Figure 3 shows the schematic structure of the reference monitor concept⁴⁴¹.

Conceptually speaking, a reference monitor is nothing more than a container for a security policy. If we “fill” this container with a certain security policy, i.e. with defined subjects, objects and relations between them (e.g., security clearances

⁴³⁶ See, e.g.: Pipkin (2000): 14; Stallings (1999): 5).

⁴³⁷ See: Bishop (2003): 574.

⁴³⁸ See: Anderson (2001): 140.

⁴³⁹ See: Anderson, Stajano, Lee (2001): 189.

⁴⁴⁰ See: Bishop (2003): 502.

⁴⁴¹ See: Stallings (1999): 530.

and classifications), it will enforce the policy (what is allowed, what is forbidden) circumscribed thereby.

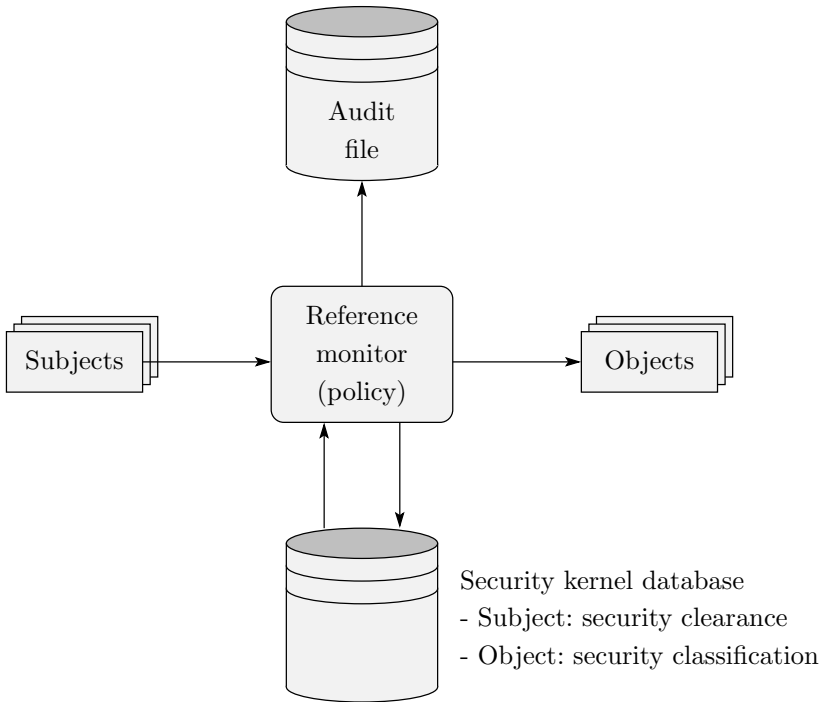


Fig. 3. The Reference Monitor Concept⁴⁴²

The implementation of a reference monitor concept is called a “reference validation mechanism” (RVM) and shows the following properties⁴⁴³: (1) It is tamper resistant;⁴⁴⁴ (2) it cannot be bypassed; (3) it is small enough for complete validation⁴⁴⁵. Around the RVM, the “trusted computing base” (TCB) is built. “A *trusted computing base (TCB) consists of all protection mechanisms within a computer system — including hardware, firmware, and software — that are responsible for enforcing a security policy.*”⁴⁴⁶

⁴⁴² Source: Stallings (1999): 530.

⁴⁴³ See: Bishop (2003): 502.

⁴⁴⁴ In fact, Bishop uses the term “tamper proof” here. For some critical analysis of so-called “tamper proof” devices, see: Anderson, Kuhn (1996/1997); Bao, Deng, Han, Jeng, Narasimhalu, Ngair (1997).

⁴⁴⁵ In practice, however, the third criterion quite often cannot be fulfilled due to “size or complexity of the reference validation mechanism”, as the Orange Book acknowledges. Nevertheless, we speak of a TCB in such cases too. Cf.

<http://www.kernel.org/pub/linux/libs/security/Orange-Linux/refs/Orange/OrangeI-II-6.html>.

⁴⁴⁶ See: Bishop (2003): 502.

According to the TCSEC (“Orange Book”), “[t]he heart of a trusted computer system is the Trusted Computing Base (TCB) which contains all of the elements of the system responsible for supporting the security policy and supporting the isolation of objects (code and data) on which the protection is based.”⁴⁴⁷

Trusted systems are built upon a TCB. According to Stallings⁴⁴⁸, a trusted system then is “[a] computer and operating system that can be verified to implement a given security policy.”

One property of the trusted system concept that might not spring to mind at first glance is its policy–neutrality.⁴⁴⁹ You can imagine almost any security policy⁴⁵⁰ that is enforced by the reference monitor as conceptualised above. Those who draft the policy and craft the code to enforce it are the ones who put the values into the system. The system will behave according to the values represented as policy and code.⁴⁵¹ This approach, however, is rather static. Typically, hardware, software, and policy as a whole are evaluated against defined criteria. A certificate attests compliance with these criteria for the system as a whole. Changing security relevant components on the fly invalidates the attestation, which means lack of flexibility to adapt to new (security) needs and goals. While being appropriate for environments with constant structures and tasks, this makes less sense for newly emerging technologies and services. With regard to new business models in a networked world, a different approach to trusted systems has been put forward by Xerox scientist Mark Stefik.

III.2 Trusted Systems According to *Stefik*

In an influential article,⁴⁵² Mark Stefik⁴⁵³ has given a new coat of paint to the old concept of trusted systems.

⁴⁴⁷ Cf. Orange Book, loc. cit.

⁴⁴⁸ See: Stallings (1999): 543.

⁴⁴⁹ But note that the policy–neutrality, while given in theory, may not be implemented in practice. Actually, due to issues of complexity and validation, most concrete trusted systems are not policy–neutral.

⁴⁵⁰ See: Schneider (2000): 30 f., defining a “security policy” as follows:

“A security policy defines execution that, for one reason or another, has been deemed unacceptable. For example, a security policy might concern access control, and restrict what operations principals can perform on objects; information flow, and restrict what principals can infer about objects from observing system behaviour; availability, and restrict principals from denying others the use of a resource.”

⁴⁵¹ Below the digital surface, the combination of digital numbers “structures and constrains social and legal power”. Moreover, we can think of code as a significant part of the institutions of the emerging information society. In the words of Douglass North (1999: 495), “Institutions are the rules of the game — both formal rules and informal constraints (conventions, norm of behaviour, and self-imposed codes of conduct) — and their enforcement characteristics.”

⁴⁵² See: Stefik (1997).

⁴⁵³ Mark Stefik was perhaps not the inventor of this “reevaluation of all values” (Nietzsche) but surely its most influential proponent. Lawrence Lessig, e.g., in his

The intention of his verbal take-over was to transform a standard computer technology into a “copyright box”⁴⁵⁴. And so he describes the new understanding for trusted systems:

*“A trusted system is a system that can be relied on to follow certain rules. In the context of digital works, a trusted system follows rules governing the terms, conditions and fees for using digital works.”*⁴⁵⁵

Stefik pursued his approach further and discusses trusted systems in the context of the Internet as:

*“systems, which protect digital works using a set of rules describing fees, terms, and conditions of use. These rules, written in a machine-interpretable digital-rights language, are designed to ensure against un-sanctioned access and copying and to produce accurate accounting and reporting data for billing.”*⁴⁵⁶

A quite simple concept designed to enforce, in principle, freely selectable security policies is thereby transformed into a concept for the enforcement of “digital rights” — “machine-governed rules of use” for content such as “[c]reative works.”⁴⁵⁷

If we try to precisely identify all the parts of Stefik’s approach to trusted systems, we can list them as follows: (a) access restriction; (b) copy restriction; (c) use control; (d) accounting; (e) reporting for billing.

In analogy to figure 3 showing the reference monitor concept, we can sketch Stefik’s design as shown in figure 4.

Two additional databases (dashed boxes) complement the database and audit file used by the reference monitor (renamed to DRM monitor for the sake of explanation). One database is needed to store the digital rights⁴⁵⁸ and one for the accounting and billing data generated during the subject’s use of protected objects.

To prevent any manipulation by the user, neither of the additional databases will be stored on the user’s system. Since the DRM monitor is at least in part managed by a source outside of the system’s boundaries, the objects are not under full control of the subjects anymore.

From the user’s point of view, the crucial issue is the concurrent implementation of two different access control mechanisms: one as described in the digital rights database and one as described in the security kernel database. According to

book “Code and Other Laws of Cyberspace”, quotes well known cryptographer Ralph Merkle with a Stefik-like statement (1999: 127). Nevertheless, many commentators consider Mark Stefik being the inventor of “trusted systems”. Cf., e.g., Griffith (1999) and Gimbel (1998).

⁴⁵⁴ See: Stefik (1999): 55.

⁴⁵⁵ See: Stefik (1997): Sect. II (A) Para. 1.

⁴⁵⁶ See: Stefik (1999): 55.

⁴⁵⁷ *ibid.*

⁴⁵⁸ For the sake of simplicity, we assume the implementation of the digital rights storage as a database. In practice, the necessary information is stored in part in a database and in part tied to the objects (e.g. as digital watermarks).

Stefik and other proponents of DRM systems, the thereby enforced DRM policy will have higher priority than the security policy under the user’s control.⁴⁵⁹

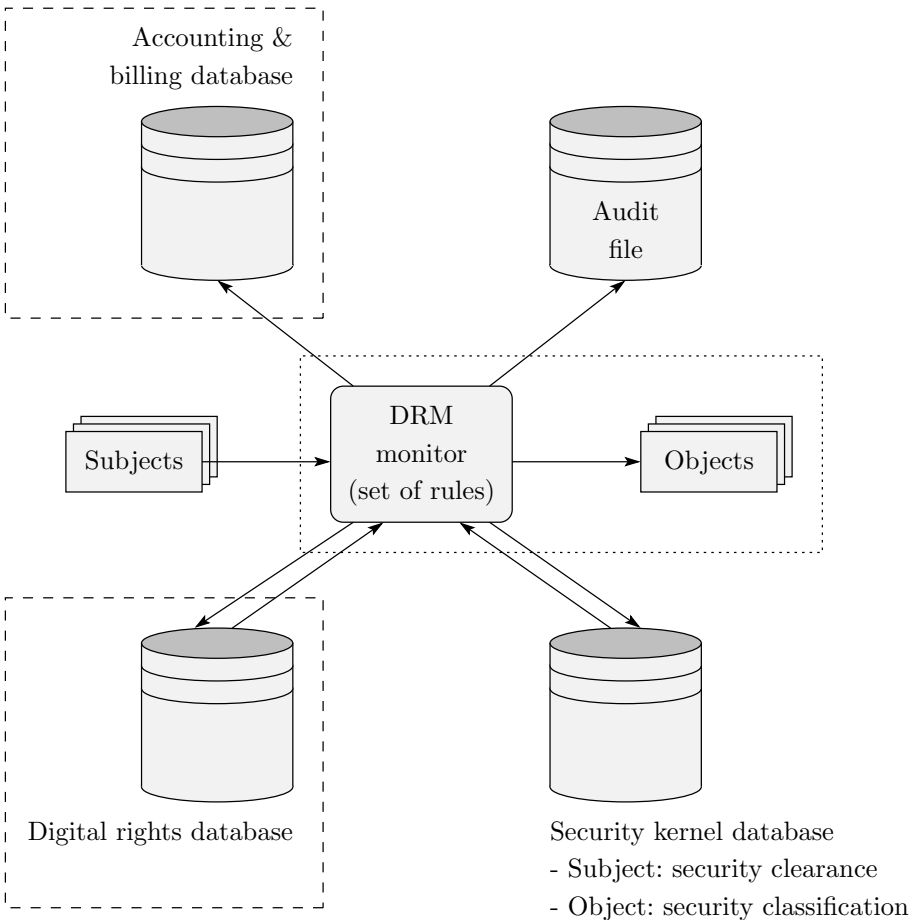


Fig. 4. Stefik’s Design for Trusted Systems⁴⁶⁰

The main difference between trusted systems designed according to the classic concept and Stefik’s trusted system is that the first ones are conceptually policy-neutral while the last one is clearly policy-specific.

Many people express their disagreement with these DRM systems by spelling them as “Digital Restrictions Management”. As long as definitions of policies addressing digital rights are not in line with copyright law as well as with reasonable user expectations regarding freedom of speech, and protection of privacy,

⁴⁵⁹ This is exactly the meaning of the laws giving legal backing to such “trusted systems”. Recent heavily disputed legislation — the Digital Millennium Copyright Act (DMCA) in the U.S., and the EU Directive 2001/29/EC in Europe — pinpoint the principle of primacy for digital rights management systems.

⁴⁶⁰ Figure based on Stallings (1999): 530.

criticism of systems built to enforce DRM will remain widespread. Nevertheless: simplistically applying the same criticism to the Trusted Computing Architecture means to overshoot the target.

III.3 From Trusted Systems to the Trusted Computing Platform Architecture

The description of trusted systems given above made a clear distinction between their (conceptually) policy-neutral and their (conceptually) policy bound appearance. How do Trusted Computing Platforms fit into this picture?

Compared to Stallings (see section II: *The classic approach to trusted systems* on page 188), Bishop⁴⁶¹ defines trusted systems from a more practical standpoint:

“A trusted system is a system that has been shown to meet well-defined requirements under an evaluation by a credible body of experts who are certified to assign trust ratings to evaluated products and systems.”

Certified authorities apply existing metrics (evaluation criteria) to an existing system (a constellation of hardware and software) in This yields a “*measure of trustworthiness, relying on the evidence provided*”⁴⁶². Since it is practically infeasible to create perfectly secure systems⁴⁶³, this measure has no absolute meaning, but reflects the relative level of faith or belief one can put in it. In the real and imperfect world, we therefore talk in terms of trust rather than those of security when making judgements systems based on this measure.⁴⁶⁴

It has already been mentioned that this approach is quite static. Changing requirements and/or modification of the system configuration that affect its security property may invalidate the assurances established in a previous evaluation process and can make it necessary to re-certify the system.

Today’s systems tend to be highly dynamic. New attributes can be added on the fly. Many of them are capable to interact: mobile phone with laser printers and cameras with computers. The requirement to continuously monitor, “measure”, and signal “fitness for purpose” (see section II: *TCPA — Motivation and approach* on page 181) goes beyond what the traditional trusted systems approach had to offer and has motivated the Trusted Platform concept.

Trusted Platforms come with small, embedded hardware elements delivering low-level functionality to the operating system and applications. Once initialised, the behaviour of these elements can not be changed other than by full reset: they can be relied upon behaving as specified. Using a very simple layer model, the architecture can be sketched as shown in figure 5.⁴⁶⁵

⁴⁶¹ See: Bishop (2003): 479.

⁴⁶² See: Bishop (2003): 478.

⁴⁶³ See, e.g.: Bishop (2003): 477.

⁴⁶⁴ There are many definitions of trust and trustworthiness and not all are consistent, whereby discussions about this topic are easily mislead. For a short description of the problem see: Anderson (2001): 9 f. The overloading of the word “trust” is confusing even for experts; some scientists argue that it will do more harm than good when applied to computer systems and transactions. For a discussion see, e.g.: Nissenbaum (1999); Friedman, Kahn, Howe (2000).

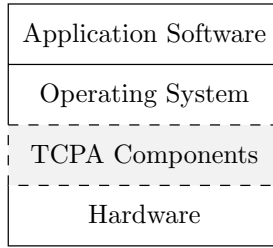


Fig. 5. A Layer Model for TCPA

The TCPA components (hardware and software) are inserted between the standard hardware and the operating system, and activated by “opt-in”.⁴⁶⁶ Taken on their own, the TCPA components do not provide more than a number of “bricks” to build a trusted computing platform⁴⁶⁷ from a conventional computer. The “mortar” comes from outside, from trusted third parties (TTPs⁴⁶⁸) that declare the trustworthiness of the “bricks”. To reflect this dependence on different stages from TTPs we enhance the above layer model. (The use of an index x for TTPs indicates the dependence from different TTPs.⁴⁶⁹)

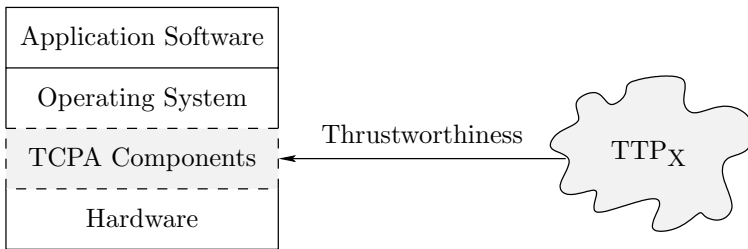


Fig. 6. TCPA Layer Model with TTPs

The layers above the TCPA layer, i.e. operating system and application software, can make use of the functionality provided in order to operate in a “trustworthy” manner. How far this goes depends on both operating system and application software. Relying on the TCPA components means: an access control policy will be enforced without unexpected interference — as long as the declaration of trustworthiness for the TCPA components holds.⁴⁷⁰ Thus, step by step, a trusted system configuration can be build up without the need to certification of the system as a whole. Compared to the classic approach to trusted systems, the trusted computing platform architecture provides much more flexibility.

⁴⁶⁵ One of the earliest descriptions of a TCPA-like architecture, the article by Arbaugh, Farber, Smith (1997), also argues along a layered approach.

⁴⁶⁶ In practice however, the borders are blurred.

⁴⁶⁷ See: Pearson, Balacheff, Chen, Plaquin, Proudler (2003): 44.

⁴⁶⁸ The trusted third parties (TTPs) are called “certification authorities” (CAs) in the TCPA terminology. See: Pearson et al. (2003): 298.

⁴⁶⁹ See *Infrastructure* in section II on page 184.

⁴⁷⁰ Due to lack of experience, it is hard to judge if this approach is feasible on a large scale.

The integration of TCPA functionality into the operating system and/or the application software requires the use of additional TTP support in order to retain the trust model. Again, certification of trustworthiness is provided by the TTP. A multi-user operating system, for example, could make use of certified identities. The integrity of system components will be certified accordingly. The actual level of trust is then derived from the level of trust before the integration of the new system component and its certificate, as shown in the next figure.

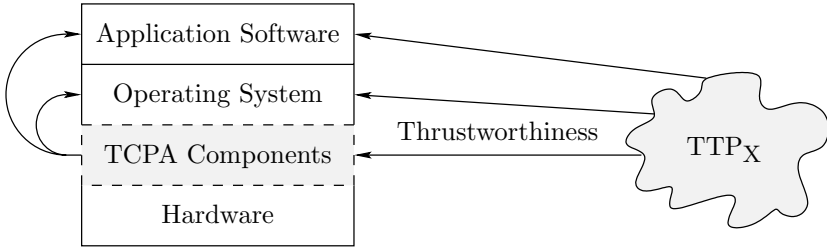


Fig. 7. Promoting Trustworthiness

Thus, trust is propagated through composition of the knowledge of an existing system configuration and authorised statements about new components. In the TCPA terminology, a “chain of trust”⁴⁷¹ is build.

In order to enable “trustworthy interaction” with other systems, the actual state of the system can be signaled to other systems. This is called “remote attestation”⁴⁷².

By evaluating this state, the remote system can decide whether the level of trustworthiness signaled by the local system is consistent with its own security policy. If the remote system decides to accept the level of trust signaled by the local system, for example, transactions initiated by the local system can take place.

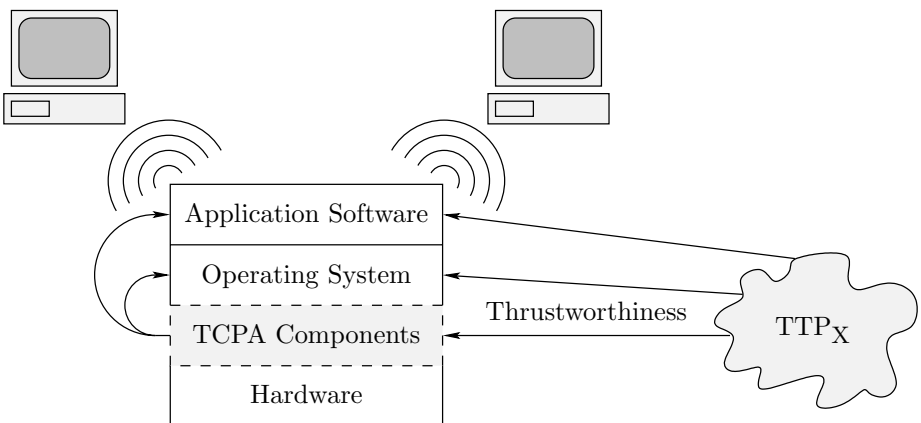


Fig. 8. Remote Attestation

⁴⁷¹ See: Pearson et al. (2003): 75.

⁴⁷² See: Pearson et al. (2003): 49.

TCPA provides “a special wrapping process that permits the caller to state the software environment that must exist in the platform before the TPM will unwrap a secret.”⁴⁷³

“Taken together, [enhanced protection of secrets and enhanced signatures] improve confidence for the owner of data that resides on remote computer systems. It becomes possible to store data on a remote computer and restrict the conditions under which that data can be used.”⁴⁷⁴

A wealth of possibilities to handle information according to different security policies is enabled by this TCPA functionality.⁴⁷⁵ There can be no doubt that DRM is one of the possibilities.

Although Pearson et. al do not explicitly refer to DRM, they write of “digital content delivery”⁴⁷⁶. “Digital content delivery” plus “restrict the conditions under which that data can be used” is a description of what DRM does. To put it bluntly, although TCPA does not define a DRM system, “trustworthy” DRM systems can be built using the TCPA components.

And here we can draw the line between DRM technology and TCPA technology. DRM technology, by definition, is policy-specific, built “to police copyright”⁴⁷⁷, while TCPA technology is conceptually policy-neutral, as was the classical concept of trusted systems before. At least from a strictly technological point of view, this statement holds.

Both proponents and opponents of DRM technology should realise this difference. When discussing the pros and cons of TCPA technology, or *whether* and *how* to regulate the deployment of this technology, the focus has presumably to be directed towards the other elements of the whole communication infrastructure: hardware, operating system, application software levels (local and remote), and certification services.

III.4 A Short Comparison of DRM and TCPA

Digital Rights Management (DRM) systems can be understood as follows:

*“Digital Rights Management (DRM) technology has emerged to protect and manage the commerce, intellectual property ownership, and confidentiality rights of digital content creators and owners as content travels through the value chain from creator to distributor to consumer, and from consumer to other consumers. In an enterprise environment, DRM is related to policy management, which controls access and management of information based on policies.”*⁴⁷⁸

⁴⁷³ See: Pearson et al. (2003): 46.

⁴⁷⁴ See: *ibid*: 47.

⁴⁷⁵ For an overview see: Pearson et al. (2003): 48–56.

⁴⁷⁶ See: Pearson et al. (2003): 7, 44.

⁴⁷⁷ See: Chris Hoofnagle in: Gaither (2002).

⁴⁷⁸ See: Duhl, Kevorkian (2001).

Based on the above made explications on the concept of trusted systems and the peculiarities of the TCPA approach, the following comparison between DRM and TCPA technology can be made:

<i>Criterion</i>	<i>DRM</i>	<i>TCPA</i>
<i>Relation to DRM</i>	is DRM	enables DRM (1)
<i>Direction</i>	“content”-centristic	“resource”-directed
<i>Policy</i>	policy-specific (enforce “digital rights” policies)	policy-neutral (enforce any access control policy)
<i>Legal status</i> (protection against circumvention)	protected by copyright laws (DMCA, Directive 2001/29/EC)	not specially protected (2)
<i>Optional</i>	(increasingly) no choice for “opt-in” or “opt-out”	specified as “opt-in” technology
<i>Hardware switch</i>	no hardware-based switch-off	hardware-based switch-off specified
<i>Standardisation</i>	different systems from different vendors (3)	standardised technology
<i>Privacy</i>	undermines users’ privacy (4)	can be used to undermine as well as to protect users’ privacy
<i>Security</i>	insecure (5)	(probably) hard to break
<i>Availability</i>	different systems available	almost ready for market (6)

Remarks

(1) DRM is one technology, and only one, that can be based on the components provided by TCPA.

(2) Since TCPA alone — as it is specified — is not capable of functioning as a “Copyright Protection and Management System” (as described in the DMCA), only *TCPA-derived technology* intended to be used as a DRM system is protected by copyright law against circumvention etc. Otherwise, by specifying a switchable “opt-in” solution, TCPA would possibly offend against the DMCA rules. Every switch disabling TCPA functionality had to be interpreted as “circumvent[ing] a technological measure that effectively controls access to a work protected under this title.”⁴⁷⁹ Additionally, TCPA will control access to computer resources that by no means, not even under the indistinct declarations of the DMCA, qualify for copyright protection.

(3) See also the article from *Chang* and *Rambhia* (discussing DRM and standardisation) in the present book on page 162.

(4) To protect users’ privacy is usually not a design goal for DRM developers, what draws continuing critique.⁴⁸⁰ Even the EU Commission, while pushing development and deployment of DRM systems, raises concerns that “[f]rom the individual’s perspective, the unlawful collection and processing of personal data

⁴⁷⁹ Title 17, United States Code, Chapter 12, §1201 (a)(1)(A).

⁴⁸⁰ See, e.g.: Cohen (2003/a).

for customer profiling and other uses by a DRM provider would constitute a threat to their privacy and could affect the willingness of consumers to accept DRMs.”⁴⁸¹.

(5) As different studies have shown, contemporary DRM systems provide only a medium level of security and, in fact, many systems do not even resist unsophisticated attacks.⁴⁸²

(6) IBM is already delivering some of its notebooks with a security chip and according software support. This *proprietary solution*, however, is not to be confused with TCPA. Nevertheless, it can be considered as some kind of a prototype of a trusted computing platform according to the TCPA specification.

IV The Future of TCPA

An updated version of the TCPA specification is currently under development. It can be expected to address well-known shortcomings of the current specification such as the simplistic audit mechanism⁴⁸³. As for the alliance itself, it has become obsolete after the formation of its successor, the Trusted Computing Group (see below).

TCPA has met a fair amount of criticism. Much of it, such as the notion of “TCPA-certified” operating systems and software, is based on misconception or mere speculation and has been dismissed as such by parties with vested interests⁴⁸⁴, but also by apparently independent analysis⁴⁸⁵. Other arguments, however, require careful consideration, not least because successful deployment of TCPA technology will critically rely on customer acceptance.

Many debates were actually centred around potential implications of “Palladium” — this is the old label for Microsoft’s efforts to build its own trusted platform (the name “Palladium” has since been replaced by the slightly more cumbersome one of “Next Generation Secure Computing Base” or NGSCB).

In the following, we give a brief overview of the Palladium / NGSCB approach and the hardware that underpins this architecture: Intel’s LaGrande technology. We will close this sections with some considerations about TCPA and Open Source and a first glimpse at the freshly founded Trusted Computing Group.

IV.1 TCPA and Microsoft’s Palladium / NGSCB

Although TCPA and NGSCB share some basic features, e.g. the TPM, Microsoft has made it clear that both have fundamentally different architectures.⁴⁸⁶

⁴⁸¹ See: EU-COM (2002): 14.

⁴⁸² See, e.g.: TÜViT (2002); EU-COM (2002); Pfitzmann, Sieber (2002).

⁴⁸³ See: Pearson et al. (2003): 71.

⁴⁸⁴ See: Safford (2002a): TCPA-QA (2002).

⁴⁸⁵ See: Anonymous (2002).

⁴⁸⁶ The following discussion is based on Microsoft’s Technical FAQ for the Next Generation Secure Computing Base. See: Microsoft Corp. (2003).

NGSCB's scope is much broader and it requires hardware support that goes far beyond what TCPA has to offer. such as those of Intel's LaGrande architecture (see below), as Intel security architect David Grawrock admitted⁴⁸⁷.

Palladium relies on a hardware component called "Security Support Component" (SSC), which has features that are very close, but not quite identical, to those offered by the TPM of TCPA. As of writing of this article (March 2003), it is still unclear whether the additional functionality required by the SSC (symmetric AES encryption) might be offered by a future version of TCPA, the chipset, the CPU, the BIOS, a combination thereof, or by a completely separate component. NGSCB creates a new environment that runs alongside the OS, the so-called "nexus". In combination with the CPU this component allows to "wall off" and hide parts of the memory from other applications and the operating system as shown in figure 9.⁴⁸⁸

According to Microsoft's FAQ, anyone can write a nexus for a nexus-aware system, users will be in control of what nexus runs on their machines, and dual-boot will be possible in the future. It is less clear, however, whether Microsoft's operating systems and nexus-aware applications will run with an arbitrary nexus, whether emulators and virtualisation layers will be affected, whether applications will employ persistent storage shielded by a particular nexus, and how attestation of applications will be obtained.

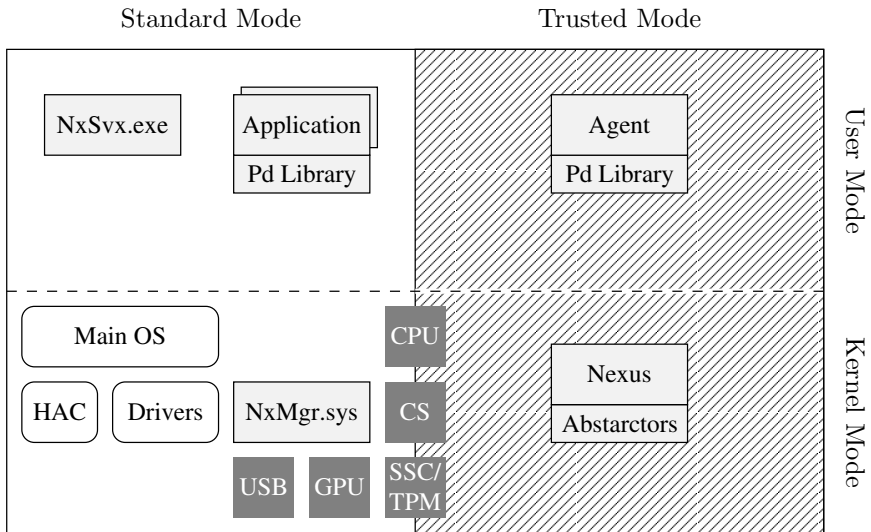


Fig. 9. MS Palladium/NGSCB Structure⁴⁸⁹

⁴⁸⁷ See: Plura (2003).

⁴⁸⁸ This figure shows the Palladium components before the concept was renamed to Next Generation Secure Computing Base. It is drawn after a picture shown in Himmelein (2003): 88.

⁴⁸⁹ Source: Microsoft.

Considered that TCPA has carefully avoided to include mechanisms for symmetric bulk encryption into the Trusted Platform Module (TPM) in order to avoid issues of export restriction, it seems quite astonishing that the SSC should contain such a capability in the first place.

IV.2 TCPA and Intel's LaGrande Processor Architecture

As of March 2003, Intel has disclosed very little information about its LaGrande architecture other than it will be released during the second half of the year⁴⁹⁰. Microsoft's plans to "wall off" parts of the memory suggests modifications of the CPU and the memory controller, e.g., by introducing a new capability that is similar, but orthogonal to the well-known "memory ring" concept of the Intel processor architecture. Secured communication between the CPU and the keyboard is likely to require support from a modified chipset.

Intel has declared that LaGrande will be an opt-in technology⁴⁹¹, at least if the new features don't find acceptance in the first place⁴⁹². This has not dispelled concerns about secondary effects such as customer lock-in and loss of privacy, in particular in conjunction with Palladium⁴⁹³. It is relatively safe to assume, though, that LaGrande can be used in conjunction with arbitrary operating systems.

IV.3 Open Source and TCPA

Whether or not TCPA leads to strengthening of customer lock-in to proprietary solutions remains to be seen. If future TCPA based software severely impedes consumers, lack of usability might actually push them to look for alternatives.

IBM as well as HP have shown commitment to both TCPA and Open Source⁴⁹⁴, and we can expect to see TCPA-supporting Linux versions hit the market in the near future.⁴⁹⁵ Both vendors will probably address the enterprise sector first. Other TCPA members declared their support for TCPA-based Linux solutions as well⁴⁹⁶.

There are, nevertheless, compelling questions about the impact of TCPA on Open Source software and its particular development model.

⁴⁹⁰ See: Ortelli (2002).

⁴⁹¹ See: Kanellos (2002).

⁴⁹² See: Bonnert (2002).

⁴⁹³ See: Gaither (2002).

⁴⁹⁴ To recall the core idea of software being "Open Source":

"The source must be available for redistribution without restriction and without charge, and the license must permit the creation of modifications and derivative works, and must allow those derivatives to be re-distributed under the same terms as the original work."

Throughout this article, we use the term Open Source in the generic manner quoted above. See: O'Reilly (1999): 34.

⁴⁹⁵ See, e.g.: Jaeger, Safford, Franke, (2002), discussing the integration of TCPA, Linux, and the Linux Security Modules (LSM).

⁴⁹⁶ See: Krill (2003).

Impact on Free and Open Source Software Developers

Since it seems reasonable to assume that the certification process for TCPA-supporting software will be neither costless, nor without expense of time, three peculiarities of the Open Source community require particular attention:⁴⁹⁷

1. Important parts (approximate 25%) of the developer community do not have significant amounts of money at their disposal. Even small charges of fees for certification may have a de-motivating effect.
2. About two thirds of the community spend between 0 and 10 hours per week developing Free and Open Source software. Every amount of time spent for certification procedures will, presumably, be deducted from the time invested for developing, testing, and debugging code.
3. Many developers are not paid for developing Open Source code. It is hard to imagine those voluntary “hackers”, i.e. sophisticated programmers with strong commitment to pushing information technology to its limits, to invest time and money in order to support business models of industry giants such as IBM and HP.

If a split of the Open Source community is to be avoided, a working model of a TCPA/OS certification process has to be shaped along the sociological structure of the community.

Impact on the GPL

A more puzzling problem is whether Trusted Platform technology will undermine the GPL and other Free Software and Open Source licences,⁴⁹⁸ destroy Free Software, allow the GPL to be “hijacked” for commercial purposes and thereby de-motivate idealistic programmers. The original argument put forward in Anderson⁴⁹⁹ is based on the notion of a “TCPA operating system” and assumptions that full use of TCPA features require proprietary certificates, neither of which is backed up by the specification. On a more general level, however, a valid point has been raised: does the attestation of security properties for Open Source software have implications for its status, flexibility, production process, and distribution?

The attestation of security properties is external to the source code and therefore not subject to the GPL. Attestation can only ever refer to a particular version of the source code: if the code is altered, the attestation of the original code loses its validity.

⁴⁹⁷ We refer to the findings of the “WIDI” study (Robles, Scheider, Tretkowski, Weber 2001) conducted by the Technical University of Berlin, Germany. A follow-up study (Ghosh, Glott, Krieger, Robles 2002) called “FLOSS” and conducted by the International Institute of Infonomics, Maastricht, The Netherlands and Berlecon Research GmbH, Berlin, Germany, showed — with minor differences — similar results.

⁴⁹⁸ See, e.g.: Arbaugh (2002): 78 f.

⁴⁹⁹ See: Anderson (2003).

Evaluators might claim that security validation of Open Source simply adds value to it. However, the validation of this very source code is only possible because it is “there” in the first place and is open to everyone. The source code to be evaluated is “there” by virtue of liberal copyright licenses that allow for a flexible development process, but the assurances that result from evaluations introduce a formerly unknown element of inflexibility. Flexibility as envisaged, e.g., by the GPL seems to be at odds with assurances provided, e.g., by a Common Criteria evaluation.

This presents a serious dilemma, as there could be clear benefits of an Open Source approach to security in general and Trusted Platforms in particular. In order to combine the flexibility of the Open Source development model⁵⁰⁰ with the growing demand⁵⁰¹ for security assurances, new technical and organisational models have to be found.

TCPA, Open Source, and Software Patents

The extent to which TCPA technology and components that can be built on top of it are protected by patents is currently unknown. As far this concerns software patents, it must be emphasised that they have long since been considered incompatible with Free/Open Source software development.⁵⁰² A “source code privilege” as proposed by Lutterbeck, Horns, Gehring⁵⁰³ could prove an essential element for enabling the integration of TCPA and Open Source software.

IV.4 The Trusted Computing Group

The formation of the Trusted Computing Group (TCG) was announced⁵⁰⁴, while we were finishing this text. The TCG has been set up as successor organisation of the Trusted Computing Platform Alliance “*to advance the adoption of open standards for trusted computing technologies*”. AMD, HP, IBM, and Intel are aboard again, as is Microsoft after temporarily having left the TCPA path. In addition, many consumer electronics companies have joined the TCG, e.g., Sony, Philips,⁵⁰⁵ and Nokia.

⁵⁰⁰ For recent advances in the field of “Open Source security” see: Ott (2003a/b); Wright, Cowan, Smalley, Morris, Kroah–Hartman (2002); Pourzandi, Haddad, Levert, Zakrzewski, Dagenais (2002).

⁵⁰¹ E.g.: from July 1st, 2002 on, all U.S. government acquisitions of IT systems processing sensitive data must be evaluated and validated according to the Common Criteria or equivalent. See: <http://www.oracle.com/corporate/press/1623351.html>.

⁵⁰² See, e.g.: Gehring (2003).

⁵⁰³ See: Lutterbeck, Horns, Gehring (2000).

⁵⁰⁴ See: Fisher (2003).

⁵⁰⁵ In fall 2001, Sony Corp. of America, Philips, and Stephens Acquisition LLC jointly bought Intertrust, holder of many trusted systems and DRM technology based patents. In the aftermath, the EU commission investigated potential negative impacts of this new joint venture for the DRM market and concluded “*that the transaction raises no serious competition concerns.*” Cf. Monti (2002): 5.

Jim Ward, chairman of the TCG, describes the aim of this organisation as follows:⁵⁰⁶

“Open standards, widely supported, will accelerate the design, use, management, and adoption of standards-based trusted systems and solutions that are urgently needed to meet the challenges of an increasingly inter-connected world.”

In order to promote this approach, the TCG will continue where TCPA has stopped.⁵⁰⁷ Microsoft is founding member of the TCG, which indicates that its NGSCB plans are compatible with whatever the TCG will pursue.⁵⁰⁸

“TCG has adopted existing trusted computing specifications from the Trusted Computing Platform Alliance (TCPA) and will extend and enhance these specifications.”

TCG and DRM?

While the TCG has dismissed any intention to develop DRM standards,⁵⁰⁹ Bill Gates has made it clear that Microsoft’s future operating systems will support DRM functionality,⁵¹⁰ and Microsoft, who considered the TCPA specification as being not comprehensive enough to support their security architecture not too long ago, has decided become a member of the TCG consortium. Given the TCG’s focus to further develop the TCPA specification, we may assume that DRM based on trusted platform technology à la Microsoft is coming closer. This time, however, it may not merely embrace personal computer systems⁵¹¹, but “multiple platforms, peripherals and devices”⁵¹² as well.

V Summary

Given the complete lack of experience with ubiquitous Trusted Platform technology, difficulties of categorisation and a shortage of independent expertise, many open questions remain. However, it is possible to summarised some preliminary observations.

TCPA and Trusted Platform technology is not identical to DRM technology, although both have a common forerunner in the Trusted Systems concept developed in the 1970s. On the other hand, TCPA offers functionality that can be a used to build DRM systems.

⁵⁰⁶ See press release “TCG announced April 8, 2003”, at:

<http://www.trustedcomputinggroup.org/home>. Last visited: 10 April 2003.

⁵⁰⁷ See TCG FAQ at: <http://www.trustedcomputinggroup.org/about/faq/>. Last visited: 12 April 2003.

⁵⁰⁸ See supra note 507. See also: ComputerWire Staff (2003).

⁵⁰⁹ See supra note 507.

⁵¹⁰ See: Schulzki–Haddouti (2003).

⁵¹¹ See: Merritt (2003).

⁵¹² See press release “TCG announced April 8, 2003”, at:

<http://www.trustedcomputinggroup.org/home>. Last visited: 10 April 2003.

Albeit members of the TCPA consortium, Microsoft and Intel appear to have staged a parallel effort to put the vision of a Next Generation Secure Computing Base into action. It is unclear whether this was a contributing factor to finally declare “[d]eath to the Trusted Computing Platform Alliance”⁵¹³ while simultaneously having the TCG raise from the ashes. Equally unclear are the consequences for a PC market already dominated by Microsoft and Intel. They could be severe, given TCPA’s wide support by the industry. Trusted Platform technology is likely to be deployed on a very wide scale. Large IT users such as big enterprises and the civil service are likely to be the pioneers here.

Microsoft’s announcement to make the source code of its nexus “widely available for review”⁵¹⁴ indicates that a huge problem might be lurking at the core of Trusted Computing: Who guards the guardians? How can one be sure that trusted software components are trustworthy indeed and not Trojan horses undermining the system’s or user’s security instead?

Combining TCPA technology with Open Source software might offer the potential to provide more trustworthiness in electronic transactions. Since the code can be subjected to scrutiny, its potential to foster trust is arguably greater than any combination of TCPA and proprietary, closed source software. The accessibility of the source code as such may not be sufficient to give a convincing answer, but its main virtue “openness” suggests itself as a necessary element to arrive at one.

The proliferation of Trusted Platform technology could change the way information technology is used. If Trusted Platform technology such as TCPA wants to be successful in delivering on its promises of bringing about more security, more privacy, and better customer confidence in electronic transactions, good answers have to be found to well-founded critique. Some of these answers may lie in imparting knowledge about the technology to the users.

In other cases, conceptual, technological or legal changes might be necessary. The Internet revolution has demonstrated that values we take for granted can quickly come under pressure in computer-mediated environments. To sustain constitutional values may well require re-regulation of technology, and it may force us to rethink intellectual property protection.⁵¹⁵

The Need for a Political Debate

Western democracies protect freedom of speech, freedom of information, freedom of trade, and other values we attribute to an open society. Technology that mediates the social discourse influences how we think about these values. Over the last years, politicians all over the world have shown remarkable reluctance

⁵¹³ See: Lemos (2003).

⁵¹⁴ See: Microsoft Corp. (2003).

⁵¹⁵ Most recently, Alan Greenspan (2003) contributed to the debate about how to put intellectual resources to most efficient use. He questioned, whether the existing system of intellectual property protection is “*appropriate [...] for an economy in which value increasingly is embodied in ideas rather than tangible capital.*”

to acknowledge this fact. Laws crafted behind closed doors and enacted to favor particular interest instead of the public one undermine the commitment of the majority of people to the “common good” (John Locke) in the long run. A broad, qualified, political debate⁵¹⁶ about how the information society is shaped by technology like TCPA and Palladium is urgently needed.

About This Document

This text documents an ongoing discussion between the authors. Should inconsistencies occur in the argumentation, they are likely to be an unavoidable result of different points of view. In many cases, we had to confine ourselves to short descriptions of important technological aspects and to forego a plethora of details.

The opinions expressed in this article are those of the authors and do not necessarily represent the positions of their employers.

⁵¹⁶ And here we do not mean a salon debate among professional politicians but rather a social discourse of all stakeholders, including the ‘users’.

2.7 DRM Under Attack: Weaknesses in Existing Systems

*Tobias Hauser, Christian Wenz*⁵¹⁷

DRM systems are insecure. This statement seems to be too simple. But like all simplifications it has a true background: Every piece of software is breakable. This chapter shows what possibilities an unfriendly intruder has and which leaks DRM systems must close in consequence. We cover audio and video protection mechanisms as well as eBooks.

I Introduction

The interesting fight between crackers⁵¹⁸ and DRM systems is not a match just for the sake of entertainment. It also has consequences in the real world. The cracker itself is not the most terrible danger. He is only one person who uses the forbidden digital right for own purposes. It gets more dangerous when he shares his knowledge on cracking with others. Everybody has access to all kinds of information via the Internet. Although crackers have to have certain knowledge and skills they can distribute their cracking knowledge in “easy to use” software tools via the Internet so that everybody can easily download these “packages” without having any cracking skills of their own. Now this is where the real problem starts.

This chapter focuses on the available cracking tools suitable for the most common formats and DRM systems like Windows Media Player and PDF, which represent the virtual goods sound, video and eBooks. The chapter also shows methods for sound and video grabbing, an alternative for the direct attack to DRM systems. The technical background of cracking tools can help to create better DRM systems and to inform users about the danger. Only when you have the knowledge you can react. The intention of giving technical background information should not be misinterpreted as a guide for crackers. It much rather intends to reveal the weaknesses of some systems in order to understand them better.⁵¹⁹

II DRM Systems in Player Software

The attacks of crackers on DRM-protected content can generally be divided into two areas: Attacks directly targeted at the key of the DRM system and circumvention methods like sound and video grabbing which attack directly in

⁵¹⁷ Hauser Wenz Partnerschaftsgesellschaft.

⁵¹⁸ Someone who breaks systems is called a cracker. Hackers are persons who have an insight-view into systems but do not destroy anything. A discussion about these two terms can be found at:
<http://www.zdnet.com/special/stories/defense/0,10459,2504308,00.html>.

⁵¹⁹ See: *Lejeune* (page 366), *Dusollier* (page 462), *Dreier, Nolte* (page 479), *Goldmann* (page 502), *Günnewig* (page 528) within this book.

front of the hardware. The attacks on the key are in the nature of today's DRM systems. Keys and licenses are provided together with the data file by the license server and stored on the user's data processor. Again, both can be attacked in two separate ways: either the attacker knows the system or parts of the system and can therefore program circumventions or the encryption is going to be directly targeted by a brute force attack which can take some time and/or process power depending on the length of the key.

Real Player and Adobe PDF are examples for DRM systems with keys and licenses stored in the data files⁵²⁰. The Microsoft DRM system which is being used by Windows Media Player works differently. Here the Media Player stores the DRM key in Windows in separate DLL files. The encryption is placed in the *blackbox.dll* data file. After personalizing the first license the data file *IndivBox.key* (also a DLL) contains a specific version of the *blackbox.dll* for the individual PC. This special version also includes the hardware ID of the PC. This topic was heavily discussed after the release of Windows XP.⁵²¹ Tests showed that implemented licenses are invalid after a change of the CPU.⁵²² In the next section you find a description of a cracking tool for Microsoft's DRM system.

II.1 Attacks on Microsoft's Audio DRM System

This section covers ways to circumvent the protection mechanisms of Microsoft's DRM system in version 1 and 2. We will show which software products exist for that task and how they work. Please note that this section is specific to Microsoft's DRM system; more general means to disable DRM will be covered in the next section.

In April 1999, Microsoft released their first Windows Media Rights Manager SDK 6⁵²³, a collection of tools for the use of the DRM functionality of the Windows Media Player (WMP). It contains Rights Manager 1, the part of the software package that enables the management of the usage rights, which the user has for a given media file (e.g., how often/long to play the file). In 2001, along with the launch of the new version 7.1 of Windows Media Player, the Windows Media Rights Manager 7 SDK was released, containing Rights Manager 7. The version number of the DRM system itself has also been increased by one: The old system from 1999 was called DRM v1, the new system is known as DRM v2.

Since DRM v2 is not backwards compatible to DRM v1, many media files that are currently offered still use DRM v1. Since the earnings of the German music industry dropped by 11.3% in 2002⁵²⁴, a trend that can be witnessed worldwide, maximizing the potential audience is a key effort. This could be one of the reasons why at the end of 2002 the US band Bon Jovi offered all registered buyers of their

⁵²⁰ See: Section "PDF and ElcomSoft".

⁵²¹ An excerpt of the discussion can be found at:

<http://www.heise.de/newsticker/data/lab-10.07.01-001>.

⁵²² See: Hauser (2003).

⁵²³ Software Development Kit, term often used for tools specifically for developers.

⁵²⁴ See: <http://www.spiegel.de/wirtschaft/0,1518,237876,00.html>.

album “Bounce” a previously unreleased track⁵²⁵ in Microsoft’s WMA format. The track could not be copied on a music CD, but three times on mobile devices that are not SDMI-compliant⁵²⁶. This track was secured using the over three years old DRM v1 system.

DRM v1

Shortly after the release of DRM v1, a software called *unfuck*⁵²⁷ emerged that could quite reliably unprotect DRM v1-secured audio files. The software itself consists of only one binary file, *unfuck.exe*; alternatively, an installation program is available that also creates a start menu and uninstall entries for *unfuck*. In order to use the software, WMA codecs are necessary. If they do not exist on the system yet, they can be found on the *unfuck* homepage itself. However, it is uncertain whether this download is legal or not.

During its first launch, *unfuck* creates an initialization file called *unfuck.ini* with the following default content:

```
[WMA Writing Output Driver]
config_waveoutdir=C:\WINDOWS\Desktop
config_bitrate=128
config_samplerate=44100
config_nch=2
```

An important value is the first parameter: *config_waveoutdir*. It contains the directory in which the unprotected media file will be saved. When you download only *unfuck.exe*, the current directory is written to the *.ini* file; with the installer distribution, the standard is the directory shown above. It is crucial to ensure that this directory exists and that *unfuck* has write access to it.⁵²⁸ If not, this entry in *unfuck.ini* can be changed after the program has been closed; after the modifications to the initialization parameters, *unfuck.ini* must be write-protected in order to preserve these settings after the next program launch.

⁵²⁵ A live version of the album’s title track, “Bounce”.

⁵²⁶ Secure Digital Music Initiative, a foundation consisting of around 160 companies. In 2000, the SDMI sponsored a challenge to try to crack their copyright protection system. A group of seven researchers from Princeton University succeeded, but when they wanted to present their findings at a conference, the RIAA (Recording Industry Association of America) reminded them that the scientists might violate the Digital Millennium Copyright Act (DMCA). See: <http://www.wired.com/news/politics/0,1283,46097,00.html>.

⁵²⁷ See: <http://go.to/unfuck>.

⁵²⁸ In particular, this is not the case under Windows NT and 2000, where the operating system usually resides in *C:\WINNT*; Windows XP has no standard subdirectory Desktop in its Windows directory. If the directory does not exist or is not writable for *unfuck*, the error messages “error playing writer” and “error creating file” is displayed.

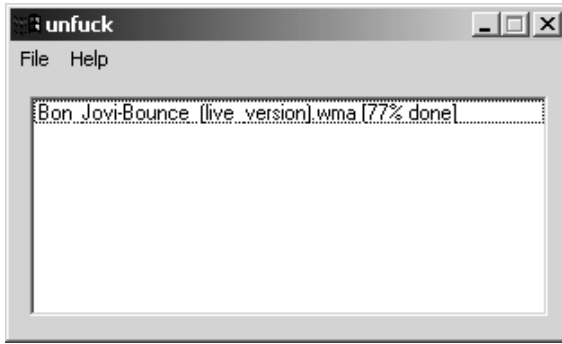


Fig. 1. The Software Unfuck (Unprotecting a Media File)

The software itself works using a very simple yet effective approach. The user must already have acquired a license for the WMA file; Windows Media Player must be able to play the file. In order to achieve that, a test within WMP (possibly including the acquisition of a license or the activation of the file) is mandatory. After that, the file may be opened within unfuck. The software now plays the file which usually would lead to a wave output of the file's contents to the speaker system of the PC. However, unfuck captures this sound output, converts it back into a — this time, unprotected — WMA file and saves it into the directory provided in the *config_waveoutdir* parameter of the *unfuck.ini* file. The new filename is the old one, however, the part before the suffix is extended by “(unfucked)”.

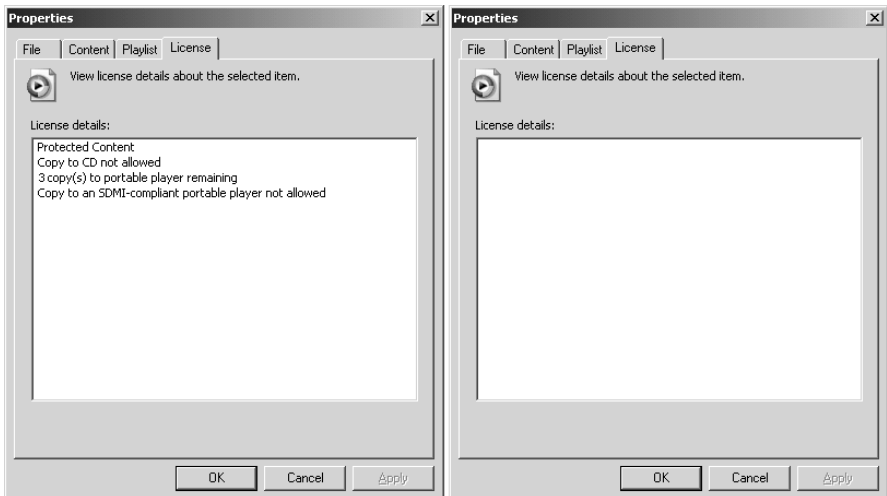


Fig. 2. The Audio File's License Information before (left) and after (right) Running Unfuck

The quality of this output (i.e. the bitrate and the sample rate of the newly created WMA file) can also be tuned in *unfuck.ini* (parameters *config_bitrate* and *config_samplerate*).

Using this mechanism, the loss of quality is minimal; the only loss of information during the process occurs during audio encoding back to WMA which is not a lossless format. Apart from that, all information is preserved, including stereo information. The resulting WMA files are not protected in any way. Unfortunately unfuck does not offer a possibility to create a lossless WAV file; section “Attacks on Arbitrary Audio DRM Systems” describes ways to achieve that.

Whereas unfuck works with all DRM v1 audio files, it fails to “unprotect” DRM v2 data; the error message “error playing file” is displayed⁵²⁹.

DRM v2

The reason for the failure of unfuck with Rights Manager 7–encoded files is that the new version creates a secured channel to the audio driver; the mechanism which unfuck uses to redirect the sound data does not work any longer. However, another approach was found which proved very effective — for some time.

The approach is often linked to the name “Beale Screamer”, a nickname apparently inspired by the movie “Network”⁵³⁰ from 1976. Peter Finch plays “Howard Beale”; the character is known for the quote “I want you to go to the window, open it, stick your head out and yell: ‘I’m as mad as hell, and I’m not going to take this anymore!’”⁵³¹.

On November 18, 2001, an anonymous poster with the self–chosen alias “Beale Screamer” sent a PGP–signed message⁵³² to the usenet group *sci.crypt*. The chosen newsgroup deals with the scientific analysis of encryption mechanisms, so it was a natural choice for the posting. The message included a technical description of how to overcome the DRM v2 copy protection, including C source code for a “proof–of–concept” program. Once compiled, an executable *FreeMe.exe* is created that allows users to unprotect DRM v2–secured audio files.

The approach by the anonymous hacker requires a valid license for the song; therefore, the software is used to artificially extended a license by creating a new version of the protected file, without any DRM restrictions.

When Windows Media Player 7.1 or higher is installed, a file called *Indivbox.key* is created. Although the file extension is *.key*, the file is a dynamic link library (DLL). The file is individualized for the current PC, so the *Indivbox.key* file differs from machine to machine. This file contains all licenses the user has acquired. All FreeMe is doing is to extract these licenses out of this file.

⁵²⁹ This error message may also occur when no suitable WMA codec is installed; however, most of the time a popup message warns the user if the codec is missing.

⁵³⁰ For more information see <http://us.imdb.com/Title?0074958>.

⁵³¹ See: <http://us.imdb.com/Quotes?0074958>.

⁵³² The message ID is 1762008I37182.4630787037@anonymous.poster; it can be viewed using Google and is also available at various mirrors, inter alia at: <http://cryptome.org/beale-sci-crypt.htm>.

This task has not been easy, and Microsoft has implemented several countermeasures, including the well-known “security through obscurity” approach. The license keys are encrypted in several ways. The positions of the license keys in the file differ from system to system. This prevents users from transferring their licenses from one PC to another one.⁵³³ In order to further increase security, the license keys are stored in the memory in the form of linked lists. This ensures that the complete key exists in memory in non-contiguous memory blocks. So it is not possible to just scan the application memory for the key.

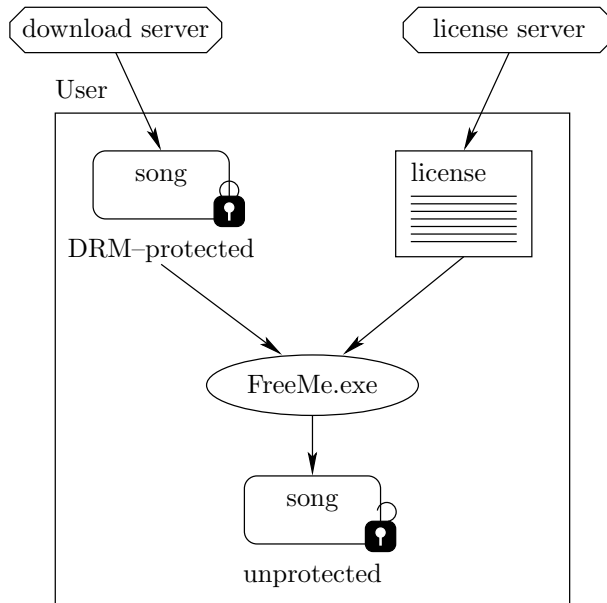


Fig. 3. FreeMe Uses the (Existing) License to Unprotect the Sound File

Another issue for “Beale Screamer” was that all communication between the various components of the WMP DRM system is encrypted, obfuscated and secured. For instance, when data shall be decrypted by the WMA system, first a temporary session key is created. The data is unscrambled, but immediately re-encrypted, this time using the session key. Thus the encryption/decryption DLL cannot be used directly; it is also necessary to reverse-engineer the session authentication and encryption mechanism. There are also other interesting aspects that obviously made it harder to crack the system: The base64 encoding sometimes uses non-standard characters, the message authentication code (MAC) used for DLL-to-DLL communication is a nonstandard algorithm⁵³⁴, apparently developed directly by Microsoft.

⁵³³ Windows Media Player includes functionality to back up licenses (menu command Tools/License Management); however, it is possible for content owners to disable this functionality for their media files.

⁵³⁴ “Beale Screamer” calls this mechanism “MultiSwap”, since the algorithm consists of numerous swap operations (exchanging two halves of a 32-bit input data).

For some time, the file *FreeMe.exe* that is retrieved by compiling the C sources succeeded in decrypting DRM v2-secured WMA files. The program loads the WMA file and uses Microsoft's WMP components to gain access to the (already existing) license. This license is used to access the sound data itself and then to write it into a new, unprotected WMA file. All other information about the file is left intact; there is also no quality loss due to a new encryption/compression of audio data as it occurs with *unfuck.exe*.⁵³⁵ FreeMe adds "Freed-" to the old file name in order to generate the new WMA.

Trying this software with a recent WMA file, however, does not work any longer. Here is a typical output of FreeMe:

```

Found DRMv2 header object.
Found KID (74321785342-01|1|128)
Found DRMv1 header object.
Starting to look for license.
License file full path:
  D:\Dokuments and Settings\All Users\DRM\drm2.lic
BlackBox library to use:
  D:\Dokuments and Settings\All Users\DRM\IndivBox.key
Keystore to use:
  D:\Dokuments and Settings\All Uers\DRM\v2ksndv.bla
Created BlackBox instance --- extracting key pairs

Public key 1 x: 6bdbae3a7518ed828816c696a01fab20a9a0f4ed
Public key 1 y: 72377a5a879511277973dbc888864d0fc34f9dbc
Private key 1: f9527926c3d854c076dcfe1b2e900fcf24bcfe7c

Checking license with PUBKEY
6bdbae3a7518ed828816c696a01fab20a9a0f4ed
Matched public key! Proceeding...
Decrypted content key is too big!

Press <ENTER> to acknowledge error.
```

The reason for that is that Microsoft has released a fix⁵³⁶ specifically for the FreeMe approach. After this patch has been applied to Rights Manager 7, all newly created, secured WMA files cannot be unprotected by FreeMe any longer. Since then, there have been no new life signs by "Beale Screamer" in *sci.crypt*; periodically, users get the "Decrypted content key is too big!" error message and complain, but it is no software fault, the reason for it has been given above.

This means that FreeMe was a technically sophisticated demonstration of a flaw in DRM v2, but there is no new version or update in sight. One of the most compelling features of this approach is that there is absolutely no loss of quality, one reason that Microsoft implemented countermeasures.

⁵³⁵ See section "Attacks on Microsoft's audio DRM system".

⁵³⁶ See:

<http://www.microsoft.com/windows/windowsmedia/wm7/drm/freemefix.aspx>.

II.2 Attacks on Arbitrary Audio DRM Systems

After the analysis of tools that were specifically written against certain versions of Microsoft’s DRM systems, this section will describe software products that make it possible to overcome any DRM system to unprotect secured audio files. The basic principle is very simple: DRM-secured systems first open and then examine secured files. If an appropriate license exists on the user’s machine, the file is started and played. The audio data are then sent to the sound card driver, which activates the sound hardware in the machine.

The software *unfuck* we described in section “*Attacks on Microsoft’s audio DRM system*” used the approach to capture the audio data on their way from the audio player to the soundcard driver. However, with DRM v2 this is no longer possible, as a secured channel is established; thus unfuck does no longer work there.

The simple, but obvious approach is now to capture the audio data on their way from the sound card driver to the hardware. In other words: A special sound card driver is written. It makes the player software believe that there is a “real” soundcard behind the driver; however, all the driver is doing is that the audio data is written to the hard disk in real-time. This ensures lossless audio data with the highest possible quality — the newly written audio files on the hard disk offer the same quality the player would have produced for the available audio hardware.

For the Windows platform there exist several products that can achieve this task. All of them implement a kind of virtual soundcard; they differ in the additional features they offer, including multi format support and audio editing capabilities. There are two different kinds of wave filters⁵³⁷: a wave capture filter takes an audio signal from a microphone or any other external source and creates a digital wave stream. A wave-rendering filter takes a digital audio stream and creates analogous (e.g. for external speakers) or digital (for instance S/PDIF⁵³⁸ output) audio data streams. Using the Microsoft technologies that are bundled with the operating system, such filters can be created. Of vital importance is DirectShow, Microsoft’s API⁵³⁹ for capturing and playing back various media data.⁵⁴⁰

There exist several software products that provide this functionality, with additional features like audio editing. Basically, most of these programs create a virtual soundcard that comes with its own drivers. These drivers offer — among other things — the possibility to directly write the audio data to the hard disk, in wave or other formats.⁵⁴¹

⁵³⁷ See: <http://www.microsoft.com/hwdev/tech/audio/highperf-driv.asp>.

⁵³⁸ Sony/Philips Digital Interface, format to transfer digital audio signals (avoiding the quality loss that occurs when converting the data to an analog format).

⁵³⁹ Application Programming Interface

⁵⁴⁰ See: <http://www.microsoft.com/Developer/PRODINFO/directx/dxm/help/ds/default.htm> for an introduction.

⁵⁴¹ Due to the enormous resources (processor power, etc.) required for encoding audio data in another format but WAV, this is not always possible or advisable, since the encoding must be done in real-time.

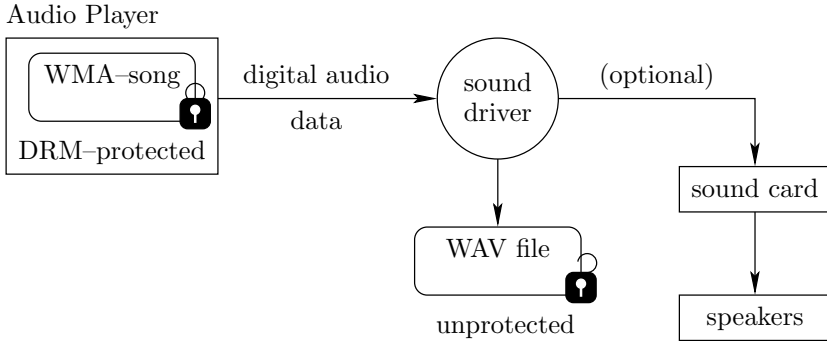


Fig. 4. The Sound Driver Writes the File to the Hard Disk

Below is a representative selection of suitable software products (as of March 1st, 2003):

- Audio Record Wizard
- SoundCapture
- Streamripper
- Super Mp3 Recorder
- Total Recorder
- Virtual Audio Cable

However, other operating systems also offer ways to capture audio data into files. Under the “old” Mac OS, that means up to version 9.x, the software MacAmp⁵⁴² offered audio capturing. Currently (March 2003) there is no full version for Mac OS X available, only a stripped-down “lite” version⁵⁴³. The full version was announced in April 2002, however, there is still no released version available yet. Since the company behind the product, Subband Software, Inc., has ceased to exist, the “full” version will most probably never appear. An alternative product that works on Mac OS X (and no previous versions) is Audio Hijack⁵⁴⁴; according to the MacAmp Lite homepage, some of the MacAmp programmers now work on this product.

Under Linux, DRM systems are not so widespread yet, mostly because of the lack of appropriate software and the “free” approach of the operating system. However, there also exist software approaches to capture audio data.

The software vsound by Erik de Castro Lopo does just that. On the project homepage⁵⁴⁵ de Castro Lopo states that he took the project offline in October 2002 due to the Digital Agenda Bill in Australia which forbids the distribution of products like vsound; however, there still exist mirrors of the original content of the page⁵⁴⁶.

⁵⁴² See: <http://www.subband.com/macamp/macamp.html>.

⁵⁴³ Available at: <http://www.macamlite.com/>.

⁵⁴⁴ See: <http://www.rogueamoeba.com/audiohijack/>.

⁵⁴⁵ See: <http://www.zip.com.au/~erikd/vsound/>

⁵⁴⁶ For instance see: <http://www.devnull.fsworld.co.uk/vsound/vsound.htm>; relevant search engines also effectively find other alternatives.

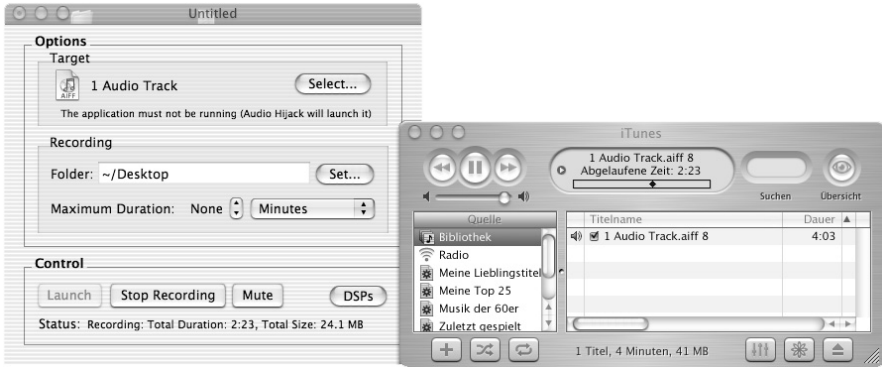


Fig. 5. iTunes is Playing the Track (right Side),
Audio Hijack is Saving the Content (left Side)

vsound uses a very simple approach: Most Linux applications that output audio data write those to the device `/dev/dsp`⁵⁴⁷. Writing to this device activates the D/A converter and produces sound output. What vsound is doing is that all access to `/dev/dsp` is intercepted and redirected to vsound. Thus, if `/dev/dsp` is first accessed, an ordinary file handle is returned, instead of the expected device handle. All subsequent `write()` calls to `/dev/dsp` write the audio data to the newly created file instead. The syntax for vsound is the following:

```
vsound -f outputfile.wav application [parameters]
```

So the following call would call Real Player (one of the few ways to play DRM-protected audio data under Linux) within vsound, input.ram is played, and is written in wave format into output.wav:

```
vsound -f output.wav realplay input.ram
```

But does it always have to be so difficult and must the audio ripping always include the usage of external software? In many cases, yes. The obvious approach, plugging a suitable hardware into the digital (S/PDIF) output of a soundcard, does not always work. For instance, recent soundcard drivers by Creative⁵⁴⁸ warn the users that the digital output of the card is shut down upon detection of audio data secured by Microsoft's DRM.⁵⁴⁹ It is a logical step that Creative's own media player (that often comes with the driver package or the soundcard) also reports to the driver if files are DRM-secured; ironically, part of many Sound-Blaster software distributions is also the software product "Creative Recorder" that enables the users to record audio data. One of the provided input sources is "What You Hear", thus making the software work like many of the programs we have described further above.

⁵⁴⁷ DSP stands for the general term "digital signal processing".

⁵⁴⁸ A company widely known for their "Soundblaster" audio card products.

⁵⁴⁹ Original text from the readme file of the Sound Blaster Live! drivers: "To protect against unauthorized duplication, Sound Blaster Live! shuts down its digital output when encrypted files are played back through a Microsoft DRM supported audio player (for example, Creative PlayCenter).".

It must be noted that all those programs and approaches not only work with DRM-protected, “static” audio files, but are also suitable for capturing streams like webradio, providing additional value to the software products.

This section showed that all protected media data can be unprotected with very little or no quality loss — since all audio data must be sent to a sound card driver, a specially constructed driver can always redirect the data to a local file. However, this also means that watermarks⁵⁵⁰ embedded into the audio files still exist, especially if 1:1 copies are created. Thus, watermarking is in our opinion the only viable option to add an almost unbreakable security to audio files. Copying and recording cannot be avoided, but it would be possible to retrieve the origin of an audio file.

II.3 Attacks on Video DRM Systems

For streaming video, by far fewer applications are available on the market, due to the much more complicated structure of the required software. CoCsoft Stream Down⁵⁵¹ promises to capture streams and download them to the hard disk. The user enters the URL of the stream (that itself is sometimes hard to find out), the software then requests the data from the server and saves them directly on the hard drive.

A more sophisticated approach is taken by the Korean software VOD Recorder⁵⁵². This program uses the Windows capturing DLL WinPcap⁵⁵³ to filter out all packages that are sent to the video player. This data is intercepted and saved on the hard drive.

Camtasia Studio⁵⁵⁴, a software primarily used to “film” the user’s actions on the PC desktop (which, in turn, is then used to create educational videos, e.g. “how to use your word processor”), which of course means that the output of the system’s video player can also be saved to disk. However, due to the special field of application of this software, the performance and resulting video quality is unsatisfying on some machines. Additionally, hardware acceleration must be turned off in order for video data to be captured, which slows down the video performance of the PC.

It can be said that video, especially streamed data, still is very secure. Whatever is displayed on the user’s monitor can be filmed and saved in certain ways, but due to the enormous amount of data to be processed and the associated potential loss of quality, this neither is an easy task nor will it be one in the near future.

⁵⁵⁰ See for more information: *Petitcolas* within this book on page 81.

⁵⁵¹ Available at: <http://stream-down.cocsoft.com/>.

⁵⁵² See: <http://www.dkcasino.com/eng/record.php3>; a very rough translation of the Korean original at <http://www.dkcasino.com/kor/record.php3>.

⁵⁵³ Additional download required; software available at: <http://winpcap.polito.it/>.

⁵⁵⁴ See: <http://www.techsmith.com/products/studio/>.



Fig. 6. The Original Stream (left) and the Captured Video by Camtasia (right)

III eBooks

One of the biggest markets for DRM-protected goods is the eBook market. In the beginning eBooks were not very popular because they were too expensive, only available on few portable devices and equipped with incompatible formats. Nowadays lots of PDAs and mobile devices are in use and on the Internet, Adobe PDF and Microsoft Reader are the most common and widely used formats. On the other hand, there are a lot of proprietary formats for portable eBooks. All these various forms and formats of eBooks were under attack of some crackers.

III.1 PDF and ElcomSoft

The most spectacular case of eBooks began during the DEFCON Nine fair in Las Vegas from July 13th until July 15th 2001. On July 16th the FBI had arrested a man in his hotel room. This man was the developer Dmitry Sklyarov, who worked for a company named ElcomSoft⁵⁵⁵. ElcomSoft is a Russian software company with headquarters in Moscow that specializes in the removal of password protection for Office documents and packed archives. One month before the DEFCON Nine ElcomSoft had introduced the new software Advanced PDF Password Recovery which is used to override several DRM restrictions of PDF formats. Sklyarov, as the head of development for this new software, spoke at the DEFCON mainly about the cracking of eBooks in general and specifically about cracking PDF.

A closer look at the software, which is available as a standard, a professional and a trial version, reveals interesting insights about methods to by-pass the protective measures of PDF data files.

⁵⁵⁵ See: <http://www.elcomsoft.com/>.

PDF data files can be provided with owner and user passwords. The standard version of Advanced PDF Password Recovery cracks owner passwords and minimizes all appending PDF rights. Thereby, safeguard mechanisms which prevent printing and/or copying of the PDF document are canceled. The professional version of the software is needed if the PDF has both an owner and user password. The user password is used for access protection whereas the owner password manages the rights of PDFs.

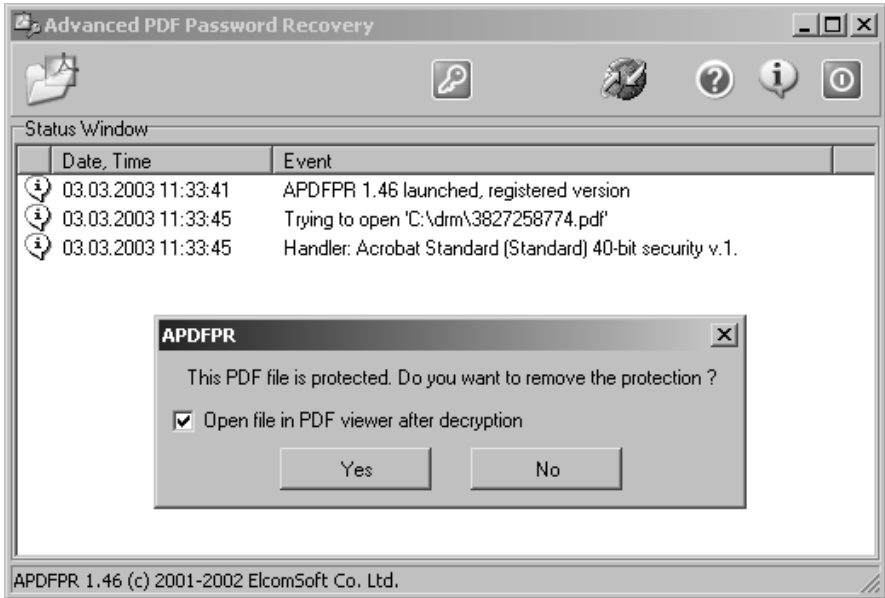


Fig. 7. The Software Advanced PDF Password Recovery

The brute-force attacks on encryption are doomed to failure with the new PDF format 1.4. The key used in this format is 128 bit long and consequently too long for trying out passwords in due time. PDF version 1.3 has only a 40 bit long key. Subsequently the 1.3 version with user password can be cracked within a few days. Of course this can be done more rapidly if there is more CPU power and more processors. The rights of a PDF without user password can be cracked immediately. For this, flags for the rights are being implemented in the PDF data file after the owner password has been cracked.

Advanced PDF Password Recovery is still (March 2003) available for download. This obviously raises the question to what happened after Sklyarov's arrest. The reason for his arrest was said to be a violation of the US DCMA (Digital Millennium Copyright Act) dated 1992. This law prohibits the development and distribution of software which purpose it is to steal intellectual property.

During the following days the situation climaxed. After rumors abounded that the founder of the PDF format, the company Adobe, had actually given the police the information which led to Sklyarov's arrest, Adobe distanced themselves

on July 23rd 2001 from the imprisonment and charges against Skylarov. Adobe stated that the developer was not the guilty party and Advanced PDF Password Recovery was not available anymore at least in the United States.⁵⁵⁶

This reaction emerged from the cooperation with the EFF (Electronic Frontier Foundation), an association which advocated the protection of freedom of a digital world. Adobe also reacted to the large number calls for protest and private initiatives⁵⁵⁷ to prevent damage to the image of Adobe.

The criminal law suite against Skylarov and his company ElcomSoft nevertheless took its course. The two defendants pleaded “not guilty”. Thereinafter Skylarov and his company parted. Skylarov made a deal with the Public Attorney’s office to end the legal proceedings but therefore had to depose against his own company. In the meantime Skylarov and the CEO of ElcomSoft had difficulties getting their visas approved to enter the United States for their appearance at court.⁵⁵⁸ But finally the hearings started. Although elaborate research was made by Adobe they could not prove that the ElcomSoft software was ever really used to crack eBooks. The federal prosecutor renounced the deposition of Skylarov but instead showed a videotape. Finally the charges were dropped. The explanatory statement confirms that the software under DCMA is illegal, but also acknowledges the fact that ElcomSoft can’t be charged with deliberate breach of this law. It is of importance in this matter that the software is actually legal under Russian law and that the economical risk would have obviously stopped a renowned company like ElcomSoft from breaking the DCMA law if they would have been aware of the consequences.⁵⁵⁹

III.2 Microsoft eBook Reader

The Microsoft format for eBooks has the extensions *.lit*. Files in this format can be read by the Microsoft eBooks Reader. The user must activate his installation of the Microsoft Reader. For this activation process the user needs a Passport account for identification. Once he has identified himself he has access to eBooks he has obtained. The DRM system for these files is also called DRM v5.

The Microsoft Reader’s DRM system has been discussed many times.⁵⁶⁰ Successful cracking attempts were reported on various news sites and in newspapers. The latest try was attempted by Dan Jackson, a programmer living in the UK.⁵⁶¹ His tool, *convert lit*, is command line-based and converts *.lit* files in such a way that they can be used on as many PCs as the user wishes. The maximum amount of PCs in the Microsoft Reader is restricted to eight. The attempt by Dan Jack-

⁵⁵⁶ See: <http://www.adobe.com/aboutadobe/pressroom/pressreleases/200107/20010723dcma.html>.

⁵⁵⁷ Exemplary <http://www.freesklyarov.org/>.

⁵⁵⁸ See: <http://www.heise.de/newsticker/data/anw-26.11.02-005>.

⁵⁵⁹ See: <http://news.com.com/2100-1023-978176.html>.

⁵⁶⁰ One example: <http://www.heise.de/newsticker/data/daa-30.08.01-000>.

⁵⁶¹ See: <http://members.lycos.co.uk/hostintheshell/>.

son to crack the Microsoft Reader-format was fear on the side of the content publishers. The trust in the Microsoft *.lit* format decreased immediately.

III.3 Portable eBooks

Most experts think that portable eBooks and their formats can be protected much better because hardware and software can interact. That may be right, but there still were some successful cracking attempts:

The best-known case is the Rocket eBook format from Gemstar.⁵⁶² In April 2001 a cracker made the information about his crack available via several newsgroup-postings after he had cracked Rocket eBooks. In the end the Internet trend magazine *Wired* wrote a widely acknowledged article about this topic.⁵⁶³

Gemstar reacted by updating the operating system of the Rocket eBook. The new version was updated in a way the users could only download eBooks from Gemstar web servers and/or eBooks submitted by Gemstar web servers. The crackers worked around this safety-feature by recovering the old operation system on newer or updated devices.

III.4 eBooks under Fire

Almost all important eBook formats have some problems with cracking tools. The question here is indeed not the fact that something happens but how to react to it properly. In all three cases mentioned above the DRM system manufacturer reacted, at least after some time, in a relatively contained manner. The content suppliers of eBooks, thus the publishers, on the other hand were considerably more frightened. Here the uncertainty spread. Non-printable books in PDF format which are distributed free of charge are being critically observed by the computer industry. Many Microsoft Reader eBooks suppliers are worried about their future after the latest successful crack attacks. Even publishers of fiction books are hesitant to produce new works of fiction as eBooks. The future will show if the suppliers of DRM system will be able to fend off cracking attempts on a continuing basis and regain the trust of the publishers.

IV Implications

Today's DRM safeguards can be circumvented, for instance with relevant tools like Advanced PDF Password Recovery from ElcomSoft or FreeMe. Furthermore, there is always the problem with grabbing the data output of sound and/or video card data.

However the here introduced tools also show the following: If the user interest of a technology or an entertainment offer has reached a certain level, it will not be long until methods to circumvent the safeguards will turn up.

⁵⁶² See: <http://www.gemstar-eBook.com/>.

⁵⁶³ See: <http://www.wired.com/news/business/0,1367,43401,00.html>.

Most of the time hackers do not work for money but for prestige. Prestige and status can be acquired best with technologies that attract a lot of interest. For this reason the Microsoft DRM system is a very interesting target for FreeMe and consequently music is the digital good that's made DRM free the most. A company like ElcomSoft does not look for prestige but even here a lot of money can be made with systems of the market leader, namely with eBooks and thus Adobe.

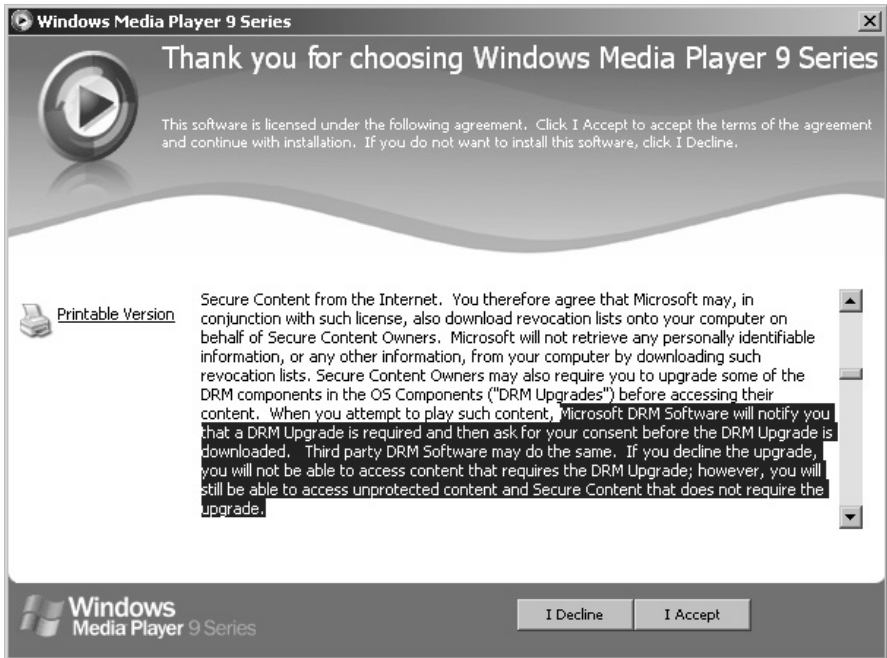


Fig. 8. Microsoft States that DRM Upgrades for new Content Could Be necessary for the Windows Media Player 9.

The image gain and the increasing publicity are certainly a welcome side effect. The remaining ElcomSoft product range, which is primarily composed of products like password recovery software for Microsoft Office products and for important data formats like zip archives, proves this fact.

If DRM systems are labeled as “easy to circumvent” it should also be mentioned that presently these systems are often one step ahead. Microsoft offers an update against FreeMe. Advanced PDF Password Recovery of ElcomSoft cannot crack the encryption of PDF 1.4 anymore or yet. In this area mostly update cycles and update possibilities for DRM systems will be of importance. Microsoft already announces the performance of automatic DRM system updates of the Windows Media Player in the accordant license agreements. These automatic updates however must be approved by the user.

The reaction time with eBooks and Adobe is longer since the content supplier has to have the latest Adobe Acrobat which is relatively expensive⁵⁶⁴. Likewise the user has to update his Acrobat Reader in case there are any changes in the DRM system.

From experience the latest version leaps caused these updates to be quite extensive and not all users execute the update right away. Consequently many eBooks are still encrypted with Adobe Acrobat 4.x

The problem with sound and video grabbing is not yet controllable in contrast to the attacks which are focusing directly on the DRM systems. The occurring loss of quality (if any) is acceptable for most music-lovers and until now there are no effective counteractive measures against crack-tools which imbed themselves as soundcard drivers.

V Helpful Crackers?

Cracking tools for DRM systems are without doubt dangerous for content and DRM system suppliers. However, before the legal club gets unpacked a peaceful approach should be sought after to make use of the know-how of the cracker or the attacking firm. A revealed circumvention always has the advantage that the attacked company can close the gap. If the company closes the gap quickly and without hesitation it will rather cause positive publicity than negative headlines. Everybody who has a certain technical interest and knowledge knows that a leading technology will always be subject to attacks.

A round table relationship between cracker and target company should not be a taboo but much rather considered as a peaceful option. Naturally the cracker should not have to be integrated into the company at once. Nobody likes to leave a burglar responsible for the alarm system, but especially for know-how and image reasons an amicable agreement should be sought after.

VI The Future

Direct attacks and brute-force attacks on DRM systems can hereafter be averted with the help of system updates. One possibility to inhibit sound and video grabbing could be a closer linkage of the DRM systems and the operating system. Microsoft pursues this path with the security initiative Next Generation Secure Computing Base (NGSCB) previously known as Palladium. This initiative uses a hardware chip according to the specification of the Trusted Computing Platform Alliance⁵⁶⁵ as technical basis.

⁵⁶⁴ Currently approx. 249 US-\$/€360; upgrade 99 US-\$/€135.

⁵⁶⁵ See: <http://www.trustedcomputing.org/>; the current version of the specification is 1.1b (<http://www.trustedcomputing.org/docs/main%20v1.1b.pdf>). *Kuhlmann, Gehring* within this book on page 178.

This alliance is a union of hardware and software manufacturers and was originally founded by Microsoft, HP, IBM, Intel and Compaq. The goal of the TCPA is to establish a security system that comprises both hardware and software. Together with the operating system the hardware chip is meant to assure the system integrity, thus protection against changes, for at least part of the system. The accordingly protected part of the PCs is also kind of a black box. To ensure the system integrity both hardware and software have to be certified. This would also be a possible solution for the sound and video grabbing problem. A piece of music that requires the highest possible security level can only be played with a certified soundcard and an appropriate driver unit. In addition the PC system should have an unprotected area which allows trouble-free download of insecure data. Until now all announcements made by Microsoft in regard to this issue are characterized by the subjects of cutting image losses against data privacy protectors and users who worry about their privacy. Technical background or beta versions are not yet available. The renaming of the Palladium into the incomprehensible acronym NGSCB was probably made to dispose of the negative term.

It is also very interesting that some declarations of Microsoft state that NGSCB is actually not meant for DRM but to protect the user's computer. For two reasons these statements don't seem plausible. On the one hand NGSCB solves the main problem of DRM systems, namely the insecure placement of the key in a data file, by relying on additional encrypting information on a hardware chip. On the other hand it allows in the same way for counteractive measures against sound and video grabbing. Neither Microsoft nor other large industry moguls will miss out on these chances for DRM systems.

If an initiative like NGSCB will however really constitute the future for DRM can not be anticipated at this point of time. It is however certain that cracker will try to overcome this challenge as well.

2.8 If Piracy Is the Problem, Is DRM the Answer?⁵⁶⁶

Stuart Haber, Bill Horne, Joe Pato, Tomas Sander⁵⁶⁷,
Robert Endre Tarjan⁵⁶⁸

I Summary

Piracy of digital content is considered a serious problem by content companies. Digital Rights Management is considered a potential solution to this problem. In this paper we study to what degree DRM can live up to this expectation. We conclude that given the current and foreseeable state of technology the content protection features of DRM are not effective at combating piracy.

The key problem is that if even a small fraction of users are able to transform content from a protected to an unprotected form, then illegitimate distribution networks are likely to make that content available ubiquitously.

One possible technological solution to the problem is what we call “draconian DRM”, which involves deploying devices that only process managed content. However, we find that such systems face significant, if not insurmountable, obstacles to deployment and we believe that the real solution to the piracy problem is largely non-technical. The most effective way for interested parties to defeat piracy may be to compete with it.

Our paper is closely related to the chapter of this book entitled: *The Darknet and the Future of Content Protection* (page 344). Instead of focusing on the distribution network, however, we describe in more depth how DRM systems attempt to deal with various aspects of piracy, and how they fail.

II Piracy

Piracy is the unauthorized use or reproduction of music, movies, books, and other types of content that are granted protection under copyright law. This kind of protection typically gives the owner of the content the exclusive right to perform certain actions on the content or to authorize others to do so. We recognize that determining whether an action is authorized or unauthorized may require protracted and subtle debate and that reasonable people may differ in their assessment of a given situation. For the purposes of this paper, however, we do not further address these subtleties, for no matter how broadly or narrowly we construe piracy we reach the same conclusion with regard to the effectiveness of DRM technologies in combating its effect.

⁵⁶⁶ The opinions expressed in this article reflect solely the view of the authors and are not necessarily the view of HP.

⁵⁶⁷ Stuart Haber, Bill Horne, Joe Pato, Tomas Sander: Hewlett-Packard Laboratories.

⁵⁶⁸ Department of Computer Science, Princeton University, and Office of Strategy and Technology, Hewlett-Packard.

There are many kinds of content that do not qualify for copyright protection because they do not contain any original authorship and are common public property. Even content that does qualify receives protection only for a limited time, after which that work becomes public property. We refer to these types of content, which are not granted copyright protection, as *public content*.

There are generally two ways in which piracy can occur:

- *Unauthorized acquisition.* The form of piracy with which most people are familiar occurs when a consumer obtains copyrighted content illegitimately, for example by unauthorized downloading of content from a peer-to-peer file sharing service such as Napster or Gnutella, or by obtaining illegitimate CDs or DVDs from a street vendor or friend⁵⁶⁹.
- *Unauthorized use.* This form of piracy occurs when a consumer obtains a piece of copyrighted content legitimately and then attempts to use it in an unauthorized way.

A fundamental flaw in the debate around DRM is that it is often assumed that a solution to the second problem will solve the first as well. In this paper we explore how various DRM technologies attempt to address these two problems, and to what extent they might succeed.

III DRM Technologies

The goal of a DRM system is to enforce licenses⁵⁷⁰ between a content provider (the licensor) and a consumer (the licensee) that define rules about authorized use of managed content. There are only a limited number of technologies that can be employed to build DRM systems to achieve this goal. These technologies can be broadly categorized as follows.

First, there must be a piece of software or hardware somewhere within the system that evaluates the license against a requested action, determines if that action conforms to the terms of the license, and either allows or blocks that action from occurring.

Second, there must be an *authentication* component to identify the licensee. The licensee could be a human user or a piece of hardware or software.

Third, we need a way to associate licenses with content. When content is associated with a license using some technological means, we say that the content is *managed*.⁵⁷¹ If content does not have a license associated with it, we say it is *unmanaged*. If users can somehow convert a managed piece of content into an unmanaged form, then they can use it in unlimited ways. In particular, they can

⁵⁶⁹ In these situations it is usually the person doing the distribution that is called the “pirate”. Since the number of illegitimate distributions must equal the number of illegitimate consumptions, we focus on the consumer side of piracy.

⁵⁷⁰ Also known as *policies* or *digital rights*.

⁵⁷¹ We could have used the term *protected* in this context, but *managed* fits more cleanly as we are making no claims as to the strength of the technological mechanism for linking content with its license.

share it with other unauthorized users. We call such illegitimately transformed content *dissociated content*.

III.1 General Vulnerabilities

Typically the license-evaluating engine executes on a computing platform that is under the control of the licensee, as opposed to the licensor. Since the licensee can potentially be an adversary, we must rely on the security of the platform to ensure that the content is used in accordance with its associated license. To buttress the security of this platform we may employ tamper-resistant hardware or software components. However, there is no widely deployed trusted platform technology that has sufficient security guarantees, and it is widely accepted within the security community that such platforms can and will be broken by determined adversaries⁵⁷².

Without authentication, an attacker could attempt to deceive the license evaluation engine into thinking that a different, authorized user is attempting to use the content. While authentication systems are well understood, they are not infallible, and thus provide another target for circumventing the system. In general, the adversary may attempt to spoof other characteristics that the license evaluation engine uses to make its decision.

In the rest of this section, we discuss how various DRM technologies attempt to bind licenses to content, how those bindings can be broken, and how these technologies attempt to deal with the problem of unauthorized acquisition. The binding can be achieved externally, by cryptographic means, using what may be called “secure container methods”; or internally, as part of the content itself, either by employing watermarking methods or by using an intrinsic property of each piece of content, as with the “fuzzy hashing” technique discussed below.

III.2 Secure Container Methods

Many DRM systems work by distributing and storing content in an encrypted form and protecting it indirectly by managing the keys used to decrypt the con-

⁵⁷² Recently much debate has arisen about the role of trusted computing platforms with regard to DRM. Much of this discussion has focused on systems such as those exemplified by the Trusted Computing Group and by Microsoft’s Palladium architecture, now known as *Next-Generation Secure Computing Base for Windows* (NGSCB). (The specification for TCG is available at: <http://www.trustedcomputinggroup.org>; for information on NGSCB, see: <http://www.microsoft.com/presspass/features/2002/jul02/0724palladiumwp.asp>.) While these technologies can be used to strengthen the delivery of ordinary DRM capabilities, we do not believe that they are effective in combating piracy. As is argued in section IV below, even a small number of motivated attackers is sufficient to enable widespread dissemination of content. Both TCPA and NGSCB are designed to be robust against software attacks on the platform, but with a focus on low costs these systems are not designed to withstand motivated physical attacks on the hardware. As a result, content manipulated on these systems can be assumed to be vulnerable to the determined pirate.

tent⁵⁷³. The license can be associated with the protected content in a variety of ways, for example as a header to the encrypted file. There is typically some attempt to “hide” the decryption keys from the user with tamper-resistant software or hardware methods. We call DRM systems based on this kind of technique *secure container methods*.

Secure container methods have a limited ability to address the piracy problem since they have no mechanisms to prevent unauthorized acquisition. They must rely on some other method to address this aspect of piracy.

Encrypting the content solves some useful problems. In particular, it allows the system to target content towards a specific device or user and prevents eavesdropping by an unauthorized party during transmission. But ultimately, we have only deferred a solution to the primary problem of preventing unauthorized use of content to that of preventing unauthorized use of the key. Consequently, we need some mechanism to manage the key in the sense above of associating it with a license.

Clearly, the licensee must eventually obtain the key to use the content. Once the key is obtained, the security of the system relies entirely on the security of the trusted platform to maintain the binding of key to content. This binding can be broken either by finding the hidden key or by modifying the license evaluation engine to release the content in an unprotected form.

Even without compromising the security of the trusted platform, there is an almost trivial approach to convert managed content to dissociated content. Content must eventually be released in an unprotected form in order for it to be consumed. Music and movies must be converted to sound waves and photons for us to enjoy it. Content can be sampled at those points in the control flow where it is no longer directly associated with a license. This problem is commonly known as *the analog hole*, because these capture points usually occur after the content has been converted from digital to analog form. But the term “analog hole” is overly restrictive, since the problem exists even while the content is still in digital form. For practical purposes, the content is often in an unprotected form in device drivers, memory, or storage long before its digital-to-analog conversion, and so can be easily captured at these points as well. Once again, we must rely on the security of the trusted platform to protect the content at as many of these points as best as we can. But ultimately there are points at which the content can no longer be protected.

III.3 Watermarking

In watermarking, a signal is embedded directly into the content; the signal is imperceptible to humans, but can be detected by machines. For the purposes of this discussion, the signal represents the license associated with the content (even though, in many cases where watermarking has been proposed, the “license” is an especially simple one or is a reference to an external license specification).

⁵⁷³ E.g., see: Sibert, Bernstein, Van Wie (1995).

We do not address here the subject of *fingerprinting*, in which the watermark represents the identity of the licensee and is typically used for forensic purposes.

Watermarking deals with the problem of unauthorized use by detecting watermarks in content and deciding whether or not the content can be used according to the license specified by the watermark. Watermarking deals with unauthorized acquisition by assuming that watermark detectors are ubiquitously embedded into all of the critical points at which content might be used.

To break the binding between the license and the content involves either removing the watermark or making the watermark undetectable. This is typically accomplished by applying basic data transformations to the content; for example, for images these transformations include scaling, cropping, and compression. The very ubiquity of the watermark detectors considerably eases the task of removing a watermark from a piece of content: an attacker can use the detector as part of an algorithm to remove the watermark⁵⁷⁴. The goal of watermarking is to make it difficult to allow these transformations to succeed without causing unacceptable perceptual distortions in the content. In fact, watermarking schemes are usually designed so that the watermarks will survive the conversion from digital to analog form. A scheme that achieved this goal would be useful in facing certain attacks via the analog hole.

Unfortunately, we cannot provide a strong security assessment of watermarking technologies. A fundamental problem with watermarking is that we only have partial theories of human perception (and we are unlikely to find one in the near future, as this is an extremely difficult artificial intelligence problem). This is a double-edged sword. On the one hand, it is this lack of understanding that gives us the ability to insert watermarks into content in the first place. If we did understand perception we could in principle compress all perceptually equivalent signals to the same value, leaving no bandwidth for watermarks. On the other hand, this lack of understanding means that we can give no strong security guarantees about watermarking because, at best, we must rely on empirical evidence to say that removing a watermark necessarily results in a perceptually degraded signal.

Moreover, it is not clear that any existing watermarking techniques achieve their stated goal. Most of the techniques described in the academic literature just address specific aspects of the watermarking problem, or they have later been shown to be vulnerable to attack⁵⁷⁵. Proprietary algorithms from technology vendors have failed to show robustness in public challenges⁵⁷⁶ or have not been widely enough deployed to evaluate their strength.

We believe that, given this state of affairs, we have to make the assumption that watermarking will not provide any significant security in the near future. Although a number of claims for the effectiveness of watermarking have been made so far the technical reality has turned out to be disappointing.

⁵⁷⁴ See: Kalker, Linnartz, van Dijk (1998).

⁵⁷⁵ See: Petitcolas (2000).

⁵⁷⁶ See: Craver et al. (2001).

III.4 Fuzzy Hashing

A relatively new alternative to secure containers and watermarking is “fuzzy hashing”, such as the Fraunhofer AudioID technology that has been developed recently for audio content⁵⁷⁷. In principle, this kind of technique could be applied to other forms of content such as video. Instead of inserting a signal into the content, as is done with watermarking, the goal of fuzzy hashing is to recognize the content directly. Unlike cryptographic hashing, where the hashes of two different pieces of data are wildly different even if the data differ by only a single bit, fuzzy hashing attempts to compute an identical hash for two pieces of content if they are perceptually equivalent. The hash value can then be used as a key to query a database for the licensing information associated with a piece of content.

There are two choices for a system architecture using fuzzy hashing. Either the hashes are stored locally with the license evaluation engine, or they are stored remotely on a centralized server. If the hashes are stored locally, the list needs to be continuously updated as new content is created. The storage requirements of such a system could be potentially massive, and the cost of the device might be significant. If the hashes are stored remotely, then it is not clear how to deal with devices that are off-line.

As with watermarking, fuzzy hashing deals with unauthorized acquisition by assuming that fuzzy hash detectors are ubiquitously embedded into all of the critical points at which content might be used.

Fuzzy hashing is also heavily dependent on our understanding of human perception. To break the binding between the license and the content requires modifying the content in some way so that the hash no longer matches the hash stored in the database. Clearly, if we had complete understanding of human perception, this kind of attack would be impossible, as we would design the hash functions to account for all perceptually equivalent versions of the content.

The robustness of these technologies is unknown. Public testing is needed to determine whether the algorithms can easily be fooled. Furthermore, a number of systems issues need to be resolved for a reliable infrastructure. Lastly, this technology needs to be very precise, yielding (almost) no false positives, to ensure that personal or business users would not find themselves in the situation that legitimate (public) content is not rendered. Thus, while fuzzy hashing is an interesting technical approach, there are too many unknowns at this time to justify significant hope for a solution in the near future.

⁵⁷⁷ See: Cremer et al. (2001).

IV Ordinary vs. Draconian DRM

We've seen that there are a variety of DRM solutions to deal with the problem of unauthorized use. None of these technologies is perfect, but one might imagine that they could be made secure enough to deter all but the most determined adversaries.

Furthermore, we have seen that watermarking and fuzzy hashing are the only technologies that deal with unauthorized acquisition.⁵⁷⁸ They must be deployed ubiquitously in order to be effective. One might imagine that the various stakeholders could come to some agreement on such technology, standardize it, and deploy it so that the vast majority of devices that deal with copyrighted content would implement those technologies.

Would these two steps be enough to stop the problem of piracy? We claim that even given the optimistic hypothesis that the above conditions held, this would have little effect on piracy. The real problem with piracy is that it takes only a small fraction of users who are capable of dissociating licenses from content to make managed content available to a significant fraction of users in unmanaged form.

The key is that even if each user only shares his or her content with a small set of other users, the content can spread throughout the distribution network rather efficiently. Moreover, skilled adversaries can turn their attack into a widely distributed tool that others who are less technically sophisticated can use, further increasing the efficiency of illegitimate content dissemination. Either way, once content is dissociated from its license, it can become widely available to all who want it.

This is why the attempts by the media and entertainment industry to shut down illegal file trading systems like Napster and Gnutella are such an important component of the industry's strategy to battle piracy. However, as is well articulated in the Darknet chapter of this book, there are a number of technical reasons why this strategy is unlikely to succeed⁵⁷⁹.

One of the reasons for this failure is that DRM, as it is ordinarily conceived, requires that devices handle both managed and unmanaged content simultaneously. We call systems built according to this principle *ordinary DRM*.

The only logical alternative is what we call *draconian DRM*, in which devices that handle managed content do not handle unmanaged content at all. Specifically, technology is embedded ubiquitously at key points in the content distribution chain, most notably in rendering devices, so that content cannot be used unless it has an associated license. We assume that licenses are issued by a trusted

⁵⁷⁸ Recall the "analog hole". Only watermarking and fuzzy hashing techniques that survive analog rendering and subsequent digital recapture can be effective. Secure container systems render their content in the clear, thereby losing subsequent control of the content.

⁵⁷⁹ See: *Biddle, England, Peinado, Willman* within this book on page 344.

authority and are hard to forge. This solves the unauthorized acquisition problem since dissociated content will not be played, by definition.

However, there are serious problems with draconian DRM. The first major hurdle is that this solution would require a complete replacement of the existing device infrastructure with DRM-enabled end devices. For the sake of argument, let us assume that such a system could be agreed upon and built.

A more fundamental problem is how such a system would handle public content. And there is also the problem of how to deal with individually generated content, such as home videos, business correspondence and other such material.

There are two solutions, each with its own set of problems.

- There could be two parallel infrastructures: one that handles managed content and one that handles all other content.
- We could require that all content, whether managed or not, come with a license.

The problem with the first approach is that the parallel infrastructure could, and probably would, be used to support dissociated content. Therefore, the managed infrastructure must offer some value to the consumer that the other infrastructure does not. This may actually be feasible, for example, if the managed infrastructure had better features or lower cost than the other infrastructure. On the other hand it is not clear that consumers would not want and that infrastructure providers would not enable those same features for unmanaged content as well.

For the second solution, the primary problem is who would issue the licenses to public or individually created content. In one scenario, this could be a centralized institution, or small set of institutions, that are globally trusted by all users. However this raises a number of issues. What should be done with content that is confidential or private? Clearly any such proposal raises a number of fundamental privacy issues. Alternatively, any content-capturing device can be certified by a manufacturer and the license for content produced by the device could be certified by the device itself. However, unless playback is limited to that single device, this only delays the problem by one step. How does the recording device reliably distinguish between copyrighted and public or individually created content?

V Competing with Piracy

Ordinary DRM will not prevent piracy, and it is questionable whether or not draconian DRM can be effective either. Legal attacks will probably never make the Darknet completely go away. One might be tempted to toss up one's hands and give up.

But perhaps we should not be so hasty. It is entirely feasible that DRM could at least partially affect piracy. The software industry is currently experiencing a 40% software piracy rate. Nevertheless, the software industry by all accounts appears to be thriving. Media and entertainment companies may face a similar challenge. If piracy could be decreased by just a few percentage points using

DRM, then this might translate into millions of dollars of otherwise unrealized revenue.

But DRM does not come without a price. First there is the cost of building, deploying and maintaining a DRM infrastructure, which will eat into whatever unrealized revenues are recovered. Second, as pointed out below⁵⁸⁰, DRM-protected content is economically less valuable than unprotected content. So deploying DRM will result in fewer sales of legitimate content, which also might offset some of the revenues gained by decreasing piracy. The question is whether or not the benefits of DRM outweigh its costs.

Regardless of whether or not DRM can be effectively used as a risk management component, we believe that content producers must regard themselves as being in competition with the pirates. As expressed by Shapiro and Varian, “*The important thing is to maximize the value of your intellectual property, not to protect it for the sake of protection*”⁵⁸¹.

A historical perspective on adjusting to new technologies is useful. Many content producers reacted with alarm at the emergence of home video recording capabilities, but today video distribution is a significant vehicle for the content distribution industry. This is not an isolated case; in fact, the growth of circulating libraries and of book publishing in England and the United States in the 18th and 19th centuries is analogous to the case of the video industry⁵⁸².

The assertion that content producers might do better by structuring their offerings as subscriptions (or a variation on that model) than according to a pay-per-view model has some backing from an economic analysis by Fishburn, Odlyzko, and Siders⁵⁸³. Modeling the situation of competing producers of mass-market information goods, and surveying the history of consumer preferences in several industries, they found that producers could achieve higher revenues through bundling, and that consumers’ strong preference for flat rates could stimulate usage.

There are several different ways in which the content and IT industries might extend their offerings to compete with piracy.

- Content management:
 - *Recommendation*: A music-service tool that would offer users recommendations for songs they might enjoy, based on the history of what they have already played, would be a considerable improvement over most current offerings, in which the only way to search for a piece of music that is completely new to you is to browse by genre. Naturally, this would be useful in other media as well as music.
 - *Organization*: Very soon, users are likely to have large personal “libraries” of content that they have accessed. New tools are needed that enable users to organize and manage their content; without such tools, their libraries

⁵⁸⁰ See: *Biddle, England, Peinado, Willman* within this book on page 344.

⁵⁸¹ See: Shapiro, Varian (1999).

⁵⁸² See: Varian, Roehl (2001).

⁵⁸³ See: Fishburn, Odlyzko, Siders (1997).

will be as unwieldy as a disorganized directory of email folders. These tools would be enormously useful for all kinds of content, no matter how the users access the content and no matter where the content itself is stored (locally on a portable device, on a server, etc.).

- Content delivery:
 - *Quality of distribution*: Legitimate content distributors are typically able to offer a higher quality of service than is available in an illegitimate distribution network.
 - *Quality of content*: Content in peer-to-peer networks is often poorly sampled, and there is an emerging threat of viruses and spam. Legitimate content can be authenticated in various ways so that consumers would be assured that they only receive official versions of the content on offer.
 - *Infrastructure*: Content distributors might arrange new partnerships with infrastructure providers, e.g. with mobile phone providers, to ensure cheap and easy access to content. It would be considerably more difficult for pirates to offer such services.
- Business models:
 - As suggested above, there is evidence that producers can profit by introducing alternate methods of charging for access to content, including subscriptions, bundling techniques, and price-discrimination schemes for access to a piece of content at different times or in different formats.⁵⁸⁴
 - In addition to bundling different sorts of offerings of their digital content, providers can link digital content to concert tickets, clothing, club memberships, and other kinds of value-added merchandising.

VI Conclusion

We pointed out that unauthorized use and unauthorized acquisition are two different aspects of piracy. A key concept is how licenses are bound to content. We saw that various kinds of DRM technology address these issues in very different ways, but that all of them have some kind of flaw that make it highly unlikely that they will be able to solve the problem of piracy. The real problem with piracy is that it takes only a small fraction of users who are capable of dissociating licenses from content to make managed content available to a significant fraction of users in unmanaged form.

We explored the concept of draconian DRM, in which devices that handle managed content do not handle unmanaged content at all. Draconian DRM could potentially be effective at eliminating piracy if it were ubiquitously adopted, but it introduces a new problem of how to handle public content.

Our conclusion is that currently proposed technical measures will not be able to completely stop the illegitimate distribution of pirated content. We believe that content producers must take steps to compete with the piracy as an alternative.

⁵⁸⁴ The pricing of different parts of a sophisticated new offering along these lines might well take into account the risk-management aspects of handling pirates' competing offerings for different pieces of content.

3 Digital Rights Management: Economic Aspects

3.1 The Basic Economic Theory of Copying

*Tobias Bauckhage*⁵⁸⁵

So far we have been discussing the technological and legal environment Digital Rights Management (DRM) is surrounded by. In this section we want to revise the basic economic principles behind DRM: why information goods are protected by intellectual property rights, what the effects of unauthorized copying in a digitally networked world are and what effects strong intellectual property rights, strong copyright enforcement and DRM-Systems might have on demand and supply of information goods.

I The Proliferation of Information Goods and Their Economic Characteristics

The term Information Age has attracted a great deal of attention over the past decade. Digitization of information (1), the proliferation of computer and telecommunication networks (2) and the broad acceptance of the world wide web (3) — as the three main drivers behind this term — have utterly influenced the way, people communicate with each other, the way knowledge is shared around the globe and the way companies are operated. As a result of this technology-driven evolution, information goods have gained an increasing relevance in our society: whether in a political, social or economical sense.

But let us start by classifying the category of goods we are focusing on. What makes information goods different from traditional goods (like bicycles and bread for example)? What makes them so fundamentally influenced by the technological changes of the Information Age?

First of all the primary substance of these goods is information, not flour (bread) or steel (bicycle): information goods are made out of information; or in other words: information is both input and output of its own production process. *Shapiro, Varian*⁵⁸⁶ define the term very broadly and more auxiliary as “anything that can be digitized — encoded as a stream of bits — that is information.” This very pragmatic definition makes the picture of a bicycle and the recipe for bread information goods — but not the bicycle or bread itself. We will work with this definition: it is simple and useful.

But besides the ability of being digitized, information goods share a number of other characteristics, which economically set them apart from other goods, and these are very important for their economic behavior and the impact, the three drivers of Information Age have upon them.

⁵⁸⁵ The Boston Consulting Group (BCG).

⁵⁸⁶ See: Shapiro, Varian (1999).

Most important for our analysis are these three: (II.1) Information goods are non rival in consumption; (II.2) Information goods are partially non-excludable and (II.3) information goods have a special cost structure.

I.1 Information Goods Are Non Rival in Consumption

Most economic goods are rival in their consumption. They are not only scarce, but they are also difficult to share — that is why the potential consumers are rivals to each other. A bicycle can normally only be ridden by one person. A bread can be shared, but every piece that is given away can obviously not be consumed by the owner himself. That is different with information goods. The bread recipe could be shared with the whole world, without reducing the utility of its initial owner.⁵⁸⁷ A music tune or a joke normally does not lose its value by being shared. In other words: the consumption of an information good by an individual *A* does not hinder an individual *B*, *C*, *D*, ... from consuming the same information good.

This characteristic of course, makes information goods difficult to control. The bicycle is controlled by the person on the pedals, the bread by the one who owns it. But what about the recipe, the music tune or the joke? Their consumption, proliferation and reproduction is highly elusive and uncontrollable.

I.2 Information Goods Are Partially Non-excludable

You can keep your surroundings from riding your bicycle by locking it. You can keep them from eating your bread by eating it completely yourself or by guarding it jealously. Public goods like national defense or clean air are much harder to keep for yourself, because they are non-excludable. Partially this is also true for information goods. It is hard for example to exclude people from the consumption of a joke or even our bread recipe. Once it is shared and no guarded secret anymore, its proliferation cannot be controlled or stopped and it is difficult to keep certain groups excluded from its consumption. The enforcement of exclusion of information goods is often difficult.

I.3 Information Goods Have a Special Cost Structure

Typically information goods are produced with high initial fixed costs and reproduced with very low marginal variable costs: producing a blockbuster movie, inventing a new pharmaceutical product or writing a best selling novel ties up much more resources than the later reproduction of the additional cinema copies, the thousands extra pills or the second printed edition of the bestseller. To produce the original can easily cost a fortune, but once you have the information good, the cost of producing and distributing each additional copy is close to zero. This implies strong economies of scale: the average unit costs per sold copy

⁵⁸⁷ Except his wish is to keep the recipe secret. Then, of course, his utility level would decrease.

decline rapidly with volume, they almost equal the initial investment divided by the number of copies.

The high initial fixed costs are also sunk costs. They are usually not recoverable in case of failure. If the blockbuster movie is a flop, there will be not much of a market for its spare copies, if the pharmaceutical innovation doesn't work, the investment cannot be recovered and when the mighty bestseller doesn't leave the book shelves, not even the raw pulp can be recovered — not to mention the author's precious time. This cost structure imposes difficulties on the markets for information goods. In a competitive environment, price competition of the producers will normally drive the market prices down to marginal costs. In case of information goods, these marginal costs are close to zero. This raises the question, how information goods at all can be sold within a competitive market and how initial investments can be recovered. *Varian*⁵⁸⁸ answers the question with:

“The market structure for most information goods is one of monopolistic competition. Due to product differentiation, producers have some market power, but the lack of entry restrictions tends to force profits to zero over time.”

As long as the producer of the original information good can thus conserve the monopolistic position, he gains from his product differentiation, he can influence the price of his product and earn back his initial investments. Over time, though, entry barriers fall, prices by competition are driven towards marginal costs and producers are driven out of the market. By the same time a new set of information goods — highly differentiated and innovative — has been introduced to the market.

But how can the producer of information goods keep this status of monopolistic power against competition? How can he keep his window of opportunity open to regain the initial investments? The answer is often: copyright protection.

II The Economic Role of Copyright for Information Goods

Basically copyright is the legal guarantee for the temporary monopoly for the creator and producer of new information goods, giving him a legally protected timeframe, in which he can use his monopolistic power to regain his initial investments and make a reasonable profit by calling prices above his marginal reproduction costs.⁵⁸⁹

⁵⁸⁸ See: Varian (1998).

⁵⁸⁹ Of course, it is simplistic to say that intellectual property rights create monopolies. Klein, Lerner and Murphy (see: Klein, Lerner, Murphy (2001)) point out, that copyright law does not as patent protection law establishes a monopoly because a copyright does not grant exclusive rights to an idea, but merely to the specific expression of an idea. Of course they are right, but the expression itself often is the differentiating element and therefore the core of the competitive edge which constitutes the temporary monopoly. Example: Edgar Allan Poe first had the idea

On a larger scale copyright constitutes the benefit of the innovator and creator of information goods and therefore acts as an incentive for the creation and production of information goods in general. Copyright laws provide a private market for an almost public good. They are a market regulative to compensate for the public good characteristics mentioned above. And as a legal institution they support and increase inventions and innovations that are made within a society. Or as Abraham Lincoln summarized it for the patent system: “*The patent system is adding the fuel of interest to the fire of genius.*”

But this is only one side of the coin. Of course the ultimate goal of copyright law should be “*the promotion, advancement and dissemination of culture and knowledge.*”⁵⁹⁰ But strong copyright protection might have exactly the opposite effect: by legally making a non-excludable information good partially excludable, copyright protection excludes those from the information good consumption, who are not willing to pay the monopolistic price⁵⁹². This — from a welfare economic perspective — simply leads to the standard deadweight loss of a monopoly: the underprovision of this information good.

In some cases, as of Britney Spears’ music, this might not be such a problem. But there are information goods that are more important to society. Think about an easy way to cure a flue or the cultural heritage of Goethe and Shakespeare? Should one corporation have control over a life saving innovation? Should one corporation control the classic masters of literature, only publishing high-end expensive hardcover editions, keeping less wealthy individuals from enjoying Hamlet and Faust? Certainly not. A Society has a high interest in these information goods spreading easily, not being artificially held at a monopolistic price.

And there is another public interest against strong copyright: information fosters information and therefore should not be limited in access. Inventions and innovations often base on an existing innovation or information good. Progress in Science, Culture and Arts to a large degree depends on the free access to existing work. For instance, if a scientific article was highly copyright protected, those who didn’t have access to the new article could not challenge its author or carry forward themselves scientific progress on its basis. If Van Gogh didn’t have access to the impressionistic paintings of his coevals, he might not have overcome this style and prepared or initialized the expressionistic movement.

Summarizing there is a general trade-off between two public concerns: the production of information goods and their dissemination within a society.⁵⁹³ The lever for this trade-off is the degree of intellectual property rights and their legal and technical enforcement. Strong intellectual property protection leads to a high variety of produced information goods but a rather low penetration in

of writing detective stories, but he certainly not had the monopoly on this idea.

But he had the monopoly on this first expression of a detective story, the short story “The Murders in the Rue Morgue” — mother to all detective stories.

⁵⁹⁰ As Depoorter and Parisi⁵⁹¹ put it, p. 454f.

⁵⁹¹ See: Depoorter, Parisi (2002).

⁵⁹² Simply meaning that the price is above the marginal costs.

⁵⁹³ See: *Günnewig* within this book on page 528.

the market, whereas a weak protection reduces the variety of innovation but increases its penetration. Or as Nordhaus⁵⁹⁴ put it: weak property rights lead to their underprovision and strong property rights lead to monopoly distortions.

As always both extremes don't seem desirable. The legal construction of "Fair use" solves this trade-off problem: it allows copying of copyrighted information goods for criticism, comment, news reporting, teaching, scholarship, and research. Such a fair use although technically forbidden by copyright law, will not be considered as copyright infringement in order to serve the ultimate rule of serving the progress of knowledge within a society.⁵⁹⁵ This can be economically reasonable if it helps to circumvent the market failure of monopoly distortion and solve the underproduction problem, supporting the dissemination of information goods without reducing the incentives for innovation and creation dramatically. Whether unauthorized copying of entertainment goods via international file sharing networks is such a case of fair use is a different question.

There are many authors claiming that intellectual property protection foremost in the U.S. has increased dramatically and pushed the public trade-off out of balance: "*Throughout the 90s, the drug, entertainment and technology industries lobbied hard to erect the strongest protections for intellectual property rights in the US history. For drugs the effective duration of patents has in some cases almost doubled to 16 years, copyright on creative works can now stretch as long as 95 years, the result of lobbying by companies like Walt Disney, which wanted to keep the 73 year old Mickey Mouse from slipping into the public domain.*"⁵⁹⁶. On the other hand, the digitization certainly has increased the impact and scope unauthorized copying can have, which will be the topic of the following section.

III The Influence of Digitization on Information Goods

The Information Age earlier has been described as the triad of three drivers: (1) digitization of information, (2) telecommunication and computer networks and (3) the broad acceptance of the world wide web. These three drivers especially have an influence on information goods and their ability of being reproduced.

The digitization of information goods simplifies its reproducibility. It reduces the reproduction costs compared to analogous forms of reproduction. A content specific carrier is not longer needed, as the carrier specific — often very costly — reproduction process. In other words: Information has been technologically liberated to its purest interchangeable form: digital data. In this dense state it is circulating and proliferating much more swiftly, rapidly overcoming barriers of time and space.

But it is not only easier and less costly to copy a digitized information good. There is additionally less difference in quality between the original version of an

⁵⁹⁴ See: Nordhaus (1996).

⁵⁹⁵ For an economical discussion on Fair Use in a networked world, see: Depoorter, Parisi (2002): 454f.

⁵⁹⁶ See: Harmon (2001).

information good and its digital copy — and even the digital copy of a copy of a copy is absolutely identical to its digital master.

Secondly, the rapid extension of computer and telecommunication networks enables a fast and inexpensive access to information from the distance. The transportation of information goods therefore becomes very inexpensive and easy. And thirdly there not only is the technical possibility to access information from the distance, but the enabling networks are also widely used. The world wide web with its millions of knots enables almost an universal access to information on a worldwide basis and therefore boosts the circulation of information. Or as Bakos and Brynjolfsson summarize the impact: “*The internet provides a ubiquitous low-cost networking, low-cost digital processing and low-cost storage of information*”.

Where does this all lead to? Obviously copying in the digital age has become much easier, qualitative and quantitative limitations of copying, that had been some kind of natural border for copy proliferation, more and more vanish. The fear of producers of information goods is, that original and copy could become perfect substitutes some day and their distribution over the internet could become incontrollable. This is almost what happened with music in file sharing networks like Napster. “*For Publishers and authors, the question is, how many copies of the work will be sold (or licensed) if networks make possible planet-wide access? Their nightmare is that the number is one.*”⁵⁹⁷

IV Economic Theory of Unauthorized Copying

As already mentioned unauthorized reproduction of information goods is not a new topic. Neither is the claim for stronger intellectual property rights or powerful technological enforcement systems like DRM. These topics have been around for ages and especially moved into the center of attention every time, reproduction innovations like the book printing machine, audio tapes, photocopying machines and VCRs were introduced to the market. Facing the current developments in the entertainment industry the discussion on unauthorized copying has been very intense during the last years. Some economists claim, that the unauthorized copying via digital networks puts the whole entertainment industry at danger. Others argue that unauthorized copying does not harm but even favors the producer of information goods — so it should be warmly welcomed. This discussion inevitably leads to the question: Do we at all need DRM-Systems?

There has been quite some economic analysis on the theory of unauthorized copying. To evaluate and understand the economic role of DRM-systems and to answer the question of its necessity, it is important to understand the economic forces acting upon unauthorized copying of information goods. This section tries to categorize the theoretical work that has been done, give an overview on the

⁵⁹⁷ See: Committee on Intellectual Property Rights and the Emerging Information Infrastructure (2000): 2.

topic and some preliminary answers on the question whether there is an economical need for DRM-systems.

Roughly one could categorize the economic analysis on unauthorized copying by moving from the outside to the inside: separating very general macroeconomic models examining the relationship between supply and demand for information goods and its welfare implications for the economy from more microeconomic articles focusing on the individual process of copying or the measures to prevent it. Additionally there has to be considered a set of subtopics closely related to unauthorized copying, like Sharing or Renting information goods⁵⁹⁸. This summary will concentrate on the microeconomic approaches, because these especially form the analytical background that is important for the focus of this book: DRM.

But let us start with a short excursion into the macroeconomic perspective and the various normative discussions following it. From the macroeconomic perspective the elementary problem of information goods — as already addressed in section II — was first articulated by *Nordhaus*⁵⁹⁹. As any non-rival good, information goods face a fundamental trade-off: weak property rights lead to their underprovision and strong property rights lead to monopoly distortions. Where an economic system respectively a society wants to position itself within this trade-off is not the topic of this article. Nevertheless one should bear in mind this general trade-off, when discussing DRM-Standards: The two extremes of the trade-off are unlikely to come but they certainly dominate the public discourse. *Romer*⁶⁰⁰ for example applies the general Nordhaus-trade-off framework on the current situation in the music industry and takes a vigorous position against stronger intellectual property rights by stating:

“It will probably reduce the variety of music that is released by firms in the music business, but the magnitude of this effect is unknown and could be small. If with the passage of time, under-provision of music looms as a serious social problem, the appropriate policy response would be to find a more efficient way to provide incentives for new recordings. [...] Even in the worst case in which the government takes no action and all of the traditional music firms go out of business, the net harm to the economy in the United States or the rest of the world would be trivial.”

Although Romer’s view is plausible, his radical conclusion is certainly not universally valid for the whole range of information goods. Again, the underprovision of Britney Spears might be bearable from an intellectual and economical point of view. But what about the economic impact of the whole entertainment industry and its related industries going out of business? Or much worse: what about the underprovision of pharmaceutical or technological innovations, which are — as scientific progress in general — based on information goods.

There is a full range of normative arguments for and against intellectual property protection, both sides impressively making their points. Obviously it is impor-

⁵⁹⁸ See: Bakos, Brynjolfsson, Lichtman (1999); Varian (2000).

⁵⁹⁹ See: Nordhaus (1969).

⁶⁰⁰ See: Romer (2002).

tant to discuss the markets for information goods separately and to determine in which market the public interest in the sharing and utilization of information goods should outweigh the economic interest of its creator. This normative discussion is truly necessary. In this article anyway, we focus on the economic forces of unauthorized copying and leave the normative interpretation together with some economic framework to the reader.

The first group of articles on unauthorized copying of information goods deals with the market for scientific journals and the role of public libraries. In this context *Ordover* and *Willig*⁶⁰¹ describe in their groundbreaking article the shared consumption problem from a welfare economic perspective and indirectly address the basic problem of unauthorized copying. Until the introduction of public libraries (and photocopying machines to copy their books and journals) there only existed a primary, private market for scientific journals. The copy price of the journal divided buyers from non-buyers. The introduction of libraries and the option to photocopy created a secondary market, on which an inferior version (the lower quality photocopy) was traded at a lower price. The producers concern in this constellation was to lose buyers of the primary market to the secondary market.

In mathematical terms each individual consumer in the model of *Ordover/Willig* is represented by her valuation for the information good. There are two levels of valuations: one is measured by B and stands for the willingness to pay for the original and the second is $B-T$, which is the valuation for the copy, equaling the valuation for the original minus the transaction costs and differences in quality of the copy.

When the individual faces a subscription price for his scientific journal of p^O , his net benefit of private subscription is $B-p^O$. When he faces cost of copying and sharing such as a library usage fee of p^C , his net benefit is $B-T-p^C$, where T again describes the inconvenience of copying and also includes the difference in quality between original and copy, and p^C describes the official transaction costs like the library usage fee and the cost of copying the original. Every individual now chooses between personal subscription and library usage according to his personal B and T , assuming p^C and p^O are given. If the individual has access to a copy she will only buy a personal original, respectively stay in the primary market for originals, if

$$B-p^O > B-T-p^C$$

She will turn to the secondary market for copies, if

$$B-T-p^C \geq 0 \quad \text{and} \quad T+p^C < p^O$$

According to *Ordover/Willig* we can differentiate the potential consumers of information goods in two different groups: the potential subscribers (with $B \geq p^O$ and $T+p^C < p^O$) and the copiers (with $B < p^O$ and $T+p^C \leq B$). This differentiation is the same we made between primary and secondary users. Of

⁶⁰¹ See: *Ordover, Willig* (1978).

course the producer is against copying if he loses buyers of the primary market to the secondary market for copies and his revenues and profits therefore decline.

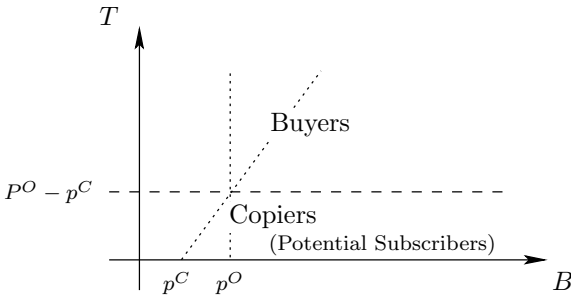


Fig. 1. The primary and secondary Users according to Ordover/Willig (1978)

But the secondary market of unauthorized copies could also have a positive effect for the producer. Economic theory offers two possibilities for this: indirect appropriability and positive network externalities.

IV.1 Indirect Appropriability

One possibility to balance the downside of unauthorized copying is — according to Ordover/Willig — a first degree price discrimination over different groups of buyers in the primary market: libraries representing several secondary journal users have to pay a multiple of the individual journal price — determined by the number of secondary users that borrow or photocopy the journal.

On the primary market the producer therefore has to price discriminate between individuals and libraries: p^{O1} for individual buyers:

$$p^{O1} = p^O$$

p^{O2} for libraries:

$$p^{O2} \leq \sum (p^C + T),$$

where p^{O2} is equal or below the sum of the individual willingness to pay of every single copier in the secondary market. A number of important articles follow this idea and compose the branch of theory summarized under the term *indirect appropriability*⁶⁰². All these articles claim, that the producers of information goods can increase their profits by encouraging unauthorized copying and adding the additional marginal willingness to pay by the secondary users on the price for the primary user and buyer of the original.⁶⁰³ The price of the original then increases with indirect usage (by copying) and the demand for originals includes the demand for copies.

⁶⁰² See: Novos, Waldman (1984); Johnson (1985); Liebowitz (1985); Besen (1986) Besen, Kirby (1989).

⁶⁰³ This of course under the assumption, that the utility and thereby the willingness to pay by the buyer rises with an increasing number of secondary users.

Novos/Waldman, Johnson and Besen examine the secondary markets for unauthorized copies mainly from a welfare economics perspective, which is for this article — centering on DRM — less enlightening. Liebowitz again analyzes in detail the determinants that influence the interaction of the primary and secondary markets for information goods and their unauthorized reproductions. According to his work, the effect of unauthorized copying depends on the relative sizes of the primary and the secondary markets, to which degree original and reproduction are substitutes for each other, the number of copies that can be produced from one original and the market specific transaction costs involved.

Starting point is the assumption, that the process of reproduction, the unauthorized copying, is controllable — or at least transparent for the producer of original information goods. This is the precedent condition of Indirect Appropriability. The producer must be able to estimate — at very low cost — the number of secondary users and their individual willingness to pay in order to set the prices on the primary market accordingly. He has to estimate the differences in quality that determine how perfect substitutes original and reproduction are. The measures of unauthorized copying have to be controllable or at least transparent.

That is the problem in our digital case. The unauthorized copying of digital information goods via digital networks is normally neither transparent nor controllable. First of all there is hardly a difference in quality between originals and their digital copies. The creator therefore might lose many primary users to the secondary market, where he cannot capture the prices paid. Additionally the digital copy now is usable as an original for further innumerable copies. In terms of Ordovery/Willig: every digital copy of a music file for example — which is not copy-protected technologically and is made accessible within a public filesharing network like Napster and its descendants — becomes something like a public library itself — open to the global online public for unauthorized reproduction at 24 hours 7 days a week. The corollary is that theoretically one single authorized master copy is sufficient to meet the full demand for this information good by unauthorized reproductions.⁶⁰⁴ That constitutes the nightmare of the industry — and shows the practical limitation of the theoretical model behind *Indirect Appropriability*.

In the case of digitized information goods it would be at least difficult for the producer to identify and price discriminate those primary buyers that let secondary users reproduce their master copies following the concept of Ordovery/Willig. In consequence producers would probably raise prices for every primary user, exceeding the willingness to pay of those primary users not sharing their master copy with others. They might then switch to the secondary market and this feedback loop would end up with very few sold copies at very high prices in the primary market and increased demand in the secondary market.⁶⁰⁵ The concept

⁶⁰⁴ Assuming that every secondary user has full access to the means of technology to download a copy of the digital information good at very low cost.

⁶⁰⁵ Still assuming that the sharing primary users would be compensated for the higher price on the primary market.

of *Indirect Appropriability* therefore is only partially applicable in the current market for digitized information goods like imagery, music or movie files. As long as open data formats like mp3 dominate the digital networks, unauthorized copying indeed seems to endanger the profits of the producer of information goods.

On the other hand theory shows the potential DRM discloses for the producers: to raise profit by allowing copying in controllable limits and indirectly capture the willingness to pay of the secondary market. Via DRM the producer could for example offer different versions of an original, that can only be copied limited times or with inferior quality. By these versions he would technologically differentiate different user segments in the primary and secondary market and could capture their willingness to pay accordingly. The theoretical work shows the main levers for DRM: the quality and quantity of the digital reproduction. DRM together with an according pricing scheme would enable the producer to price discriminate the primary users and take advantage of the concept of *Indirect Appropriability*.

Closely related with the concepts of Indirect Appropriability are the articles about Sharing and Renting⁶⁰⁶. Bakos, Brynjolfsson, Lichtman argue that Copying and Sharing of master copies in small groups of users advantages the profit maximizing producer. Via Indirect Appropriability the producer can not only set higher prices on the primary market, but with certain sharing groups there will be a favorable smoothing of the individual willingnesses to pay. In contrast to *Liebowitz*⁶⁰⁷ and *Besen*⁶⁰⁸ the authors do not assume the same willingness to pay but they set the price on the primary market equal to the sum of the individual willingness to pay of every single secondary users. Therefore small groups facilitate price discrimination. *Varian*⁶⁰⁹ states that the producer of information goods in general will sell less master copies at a higher price, if sharing or copying is possible.⁶¹⁰ Anyway this would make the producer better off, as long as (a) the transaction costs of sharing are lower than the marginal production cost of originals (e.g. car rentals), (b) the transaction costs of sharing are low and every buyer uses the product only once or twice (e.g. video rentals) or (c) a clear segmentation exists between high price buyers in the primary and low price buyers in the secondary market and enables a clear price discrimination.⁶¹¹

But as Indirect Appropriability in general, the concept of *Bakos, Brynjolfsson, Lichtman*⁶¹² is only partially true in our digital case. Fundamental for their analysis are small groups within the decision to buy and share a master copy is made collectively. This might be right for the traditional private copying case

⁶⁰⁶ See: Bakos, Brynjolfsson, Lichtman (1999); Varian (2000).

⁶⁰⁷ See: Liebowitz (1985).

⁶⁰⁸ See: Besen (1986).

⁶⁰⁹ See: Varian (2000).

⁶¹⁰ Varian (2000) does not make any difference in his work between different forms of co-usage by non-buyers, like copying, renting or sharing.

⁶¹¹ See: Varian (2000): 485f.

⁶¹² See: Bakos, Brynjolfsson, Lichtman (1999).

— where a family or group of friends buy an original and share and copy it among each other.⁶¹³ But it is certainly different in groups formed by digital networks like the file sharing networks the entertainment industry is so scared of. And even if the sharing groups had the right size and the decision processes described by theory, it would not be transparent for the producer. He could not spot the different sized sharing groups and price them accordingly.

IV.2 Positive Network Effects

There is one other group of articles claiming unauthorized copying would advantage the producer of the copied information goods: the analytical framework by *Nascimento, Vanhonacker; Conner, Rumelt; Takeyama; Slive, Bernhardt and Shy, Thisse*⁶¹⁴: they also argue that the increasing unauthorized copying will drive up the willingness to pay on the primary markets for originals.⁶¹⁵ The authors call it positive network externality or a positive network effect on demand⁶¹⁶ — according to the network–literature of *Farell, Saloner; Katz, Shapiro and Besen, Farell*.⁶¹⁷ They see information goods as services that are closely related to networks.⁶¹⁸ A positive network effect according to *Katz, Shapiro*⁶¹⁹ exists, if the utility level of a certain good increases by its number of users. The authors identify three possible reasons for this: (1) a direct physical effect of the number of users on the quality of the network good (e.g. Telephone lines), (2) the indirect effect, the number of users has on the variety of complementary goods (e.g. hardware levels determining the variety of compatible software available), and finally (3) the indirect effect the number of users has on quality and quantity of offered related services (e.g. repair services).⁶²⁰ For many information goods (e.g. standard software) one or more of these reasons are true. The group of authors on positive network effects now apply network economic theory to the area of information goods and the optimal level for copyright protection.

The basic principle these different articles are based on, has been well described by *Conner, Rumelt*⁶²¹ who applied their model to the software industry.⁶²² They

⁶¹³ This in matter of fact is also covered by the concept of “Fair Use”.

⁶¹⁴ See: Nascimento, Vanhonacker (1988); Conner, Rumelt (1991); Takeyama (1994/1997); Slive, Bernhardt (1998); Shy, Thisse (1999).

⁶¹⁵ See: Conner, Rumelt (1991): 125; Takeyama (1994): 155.

⁶¹⁶ Both terms are often used as synonyms although they are quite different in their meaning (for a more precise differentiation see: Liebowitz/Margolis (1994): 135ff.

⁶¹⁷ See: Farell, Saloner (1985); Katz, Shapiro (1985); Besen, Farell (1994).

⁶¹⁸ According to Economides (1996): 674: networks are “[...] composed of links that connect nodes. It is inherent in the structure of a network that many components of a network are required for the provision of a typical service”; telecommunication–, computer– and traffic networks are typical examples, see also: Economides (1996): 675f.

⁶¹⁹ See: Katz, Shapiro (1985).

⁶²⁰ See: Katz, Shapiro (1985): 424.

⁶²¹ See: Conner, Rumelt (1991).

⁶²² Almost all articles are on the software industry where positive network effects are especially obvious.

state, that for the positive network effect of increasing user base on the utility level of the software product, it is completely irrelevant whether the additional users have bought an original or use an unauthorized copy. A low level of copyright protection is optimal for the producer, if copyright protection has no positive effect on demand on the primary market and positive network effects on demand exist. A low level copyright protection then does not shift primary users to the secondary market, therefore does not decrease sales on the primary market, but increases the willingness to pay and therefore the potential price on the primary market according to the overall increased number of users (buyers and copiers). In other words: buyers stay and pay more. Vice Versa a high level of copyright protection is optimal, if only low network effects exist and it prevents primary users from switching to the secondary market.

*Takeyama*⁶²³ in her model pushes this idea even further. She shows, that even if all consumers on the secondary market for copies by strong copyright laws were pushed to become buyers on the primary market, the copyright protection therefore had positive effects on the demand on the primary market, the profit of the producer could still be higher with a weaker set of protection. Let us take a closer look on her model:

The Model is based on two groups of consumers. Every group has a demand function for the information good X , given by the maximum willingness to pay $V(N)$. Group N^H has a high maximum willingness to pay $V^H(X)$, and group N^L a lower $V^L(X)$. The willingness to pay is additionally depending on the total number of consumers of the information good X , therefore $\frac{dV}{dN} > 0$. In the case of monopoly under the marginal costs of production c two options for the monopolist exist: he can either set his price equal to the maximum willingness to pay of group N^H and then only this group buys his product or he can set the price equal to the lower willingness to pay by group N^L including the positive network effect at $V^L(N^H + N^L)$ and both groups will buy. The profit for the monopolist in both options is calculated by:

Option 1: Maximum protection, high price, only group NH buys

$$(1) \quad \Pi^H = N^H [V^H(NH) - c]$$

Option 2: Maximum protection, low prices, both groups buy

$$(2) \quad \Pi^L = (N^H + N^L) \cdot [V^L(N^H + N^L) - c]$$

Depending on the marginal costs c , the size of both groups and the actual amount of the willingness to pay, the monopolist either chooses option 1 or 2.

Next Takeyama lowers the protection standard and lets unauthorized copying enter her model. The copy in her model is of inferior quality to the original, the maximum willingness to pay for it thus is lower than for the original: $\alpha \cdot V(N)$, (with $0 < \alpha < 1$) describing the quality discount between original and copy (showing to which degree original and copy are perfect substitutes). Both groups

⁶²³ See: Takeyama (1994).

of consumers now can either buy the original at the price p^O , consume a copy at the price (resp. cost) of p^C or not consume the information good at all. For the monopolist's profits this means:

Option 3: Low protection, high price, group N^H buys, group N^L copies

$$(3) \quad \Pi_C^H = N^H \cdot [(1 - \alpha)V^H (N^H + N^L) + p^C - c]$$

Option 4: Low protection, low prices, both groups buy

$$(4) \quad \Pi_C^L = (N^H + N^L) \cdot [(1 - \alpha)V^L (N^H + N^L) + p^C - c]$$

Which of these options is best for the monopolist? If the producer only wants to sell to the group N^H with the higher willingness to pay, therefore sets a high price (*Option 1 and 3*), then his profit is higher where he can get a higher price. With strong network effects ($V^H (N^H + N^L) \gg V^H (N^H)$) and a high quality difference between original and copy ($\alpha \approx 0$) the monopolist maximizes his profit with a low standard of copyright protection (*Option 3*). If the difference in quality is low ($\alpha \approx 1$) and the network effects are weak ($V^H (N^H + N^L) \approx V^H (N^H)$), a higher standard of protection will maximize his profits (*Option 1*).

If the monopolist sets low prices, so that both groups buy on the primary market (*Option 2 and Option 4*), a low copyright protection always decreases profit, because copying reduces the willingness to pay of group NL and therefore also the maximum unit price, at which both groups buy. This lower price does not get compensated by the positive network effect because the maximum effect was already reached without copying. The lower price, thus the producer will only choose, if copyright protection is high (*Option 2*).

What if the monopolist can chose between *Option 2* (high protection, low price) and option 3 (low protection, high price)? In this case, Takeyama claims, the monopolist would chose option 3, if the maximum price of Group N^H increased by the positive network effect leads to a higher revenue than the overall revenue with both groups and a smaller price. The revenue differential is driven by differences in the maximum willingness to pay of group N^H and N^L and by the degree of positive network effect.

The monopolist, of course, does not make any profit, if both groups will decide to copy instead of buying the original. This scenario occurs, when the net utility level of a copy for group NH is higher than the net utility of an original:

$$\alpha V^H (N^H + N^L) - p^C \geq V^H (N^H + N^L) - p^O$$

This scenario could emerge when original and copy are perfect substitutes ($\alpha \approx 1$) and the price of a copy is very low ($p^C \approx 0$) or at least relatively low to the price of an original . In this case, obviously, strong copyright protection is the better choice for the producer.

How does the concept of positive network effects apply to our digital case? First of all the whole concept of *Conner, Rumelt, Takeyama* and others is based on the existence of network effects. Their theoretical work focuses on the software

industry and obviously this is often a good example for the existence of network effects. The value of a Microsoft Windows application for an individual certainly increases with the number of other users, allowing him to share data with them in a standard format. But that is certainly not true for all information goods: for many information goods the three drivers of positive network effects, identified by *Katz, Shapiro*, do not apply. Although one could argue, that fashion causes also a slight network effect on entertainment goods like music and film⁶²⁴, it is definitely not as practically important as in the case of standard software. And there are other markets, in which positive network effects are even more unlikely.⁶²⁵

But even if there were positive network effects in all information good markets, there is one main limitation according to Conner/Rumelt and all the others: as mentioned in section III: The three main drivers of digitization make original and unauthorized copy almost identical by simultaneously decreasing their reproduction costs and therefore the price on the secondary market. Under the assumption of low transaction costs and perfect information this means, that all — or at least many — of the users of the primary market would switch to the secondary market, where the (almost) same product is available at a lower price (reproduction plus transaction costs).

Takeyama's framework in this case effects supports the position for strong copyright protection. A high level of copyright protection seems optimal, because network effects are rather low and copyright protection prevents primary users from switching to the secondary market. The network approach does not, however support the claim for "zero tolerance" copyright protection. It shows that not unauthorized copying is the problem, but the new characteristics of digital reproduction of information goods. Especially the identical quality of original and copy prevents potential positive network effects. If the unauthorized copying did not lure primary users to the secondary market, secondary users who could not afford the product on the primary market would by unauthorized copying raise the value of the consumption of every single information good consumed — authorized or unauthorized. As long as the unauthorized copying could be controlled and limited to the non-buyers it would set the producer better off than a "zero tolerance" protection level.

V Conclusions

After revising the basic economic principles behind copying, we now are able to give some preliminary answers to the question whether DRM systems are necessary and helpful from a producer's perspective and what impact they could have on the demand and supply of information goods.

First of all one should always bear in mind, that any form of new copyright protection is shifting the current balance within the trade-off described in section

⁶²⁴ If the majority of a peer group listens to Britney Spears, the minority might be willing to pay more for a Britney CD for themselves.

⁶²⁵ For a detailed analysis of the movie industry see: Bauckhage (2002).

II: between the two public concerns of producing and innovating the necessary variety of information goods and enabling their dissemination within society. This trade-off has to be thoroughly examined and publicly discussed in every market for information goods separately. Too rigorous DRM-systems could interfere with public interest in some cases and no protection of copyright could destroy branches of the industry.

Besides this rather normative public perspective, this text examined the necessity of copyright protection from the producers perspective. The general literature on unauthorized copying makes a strong case for weak copyright laws because unauthorized copying not only serves the public interest of dissemination of information but also maximizes the profits of the producers and therefore increases the incentives for innovation. The argumentation is straightforward and unchallengeable. Nevertheless in the context of the Internet the situation seems to be slightly different.

The three drivers of the *Information Age* (1) digitization of information, (2) telecommunication and computer networks and (3) the broad acceptance of the world wide web have changed and could further change the environment in which information goods are shared and copied. They make copying, sharing, distributing and storing information almost costless and by the same time have made copy and original of an information almost good perfect substitutes. Unauthorized copying could potentially lose its natural limitations of time, space and volume and therefore truly endangers the profit of the producers — the traditional economic incentive to innovate. No copyright protection therefore would not only reduce the producers chance for profits but also the economical incentive to innovate. Most of the economical arguments for weaker protection in the digital age seem to lose their validity.

On the other hand, economic theory shows that even from a strict producers' view a "Zero Tolerance" DRM-System would not be the optimal scenario. *Indirect Appropriability*, Sharing concepts and positive network effects show, that with the right price and product differentiation, the producer could increase his profits allowing unauthorized copying in certain limitation. And from this angle, DRM could be a big chance to find a new balance within the public trade-off. DRM enables differentiation and therefore could help to fulfill differentiated needs. By controlling the dimensions of copying it could not only increase the profit of the producer but also enable fair use and even support the dissemination of information in defined limits. Of course, in order to serve the public interest these DRM standards should be thoroughly examined and even regulated by competition law.

3.2 Facing the Music: Value-Driven Electronic Markets, Networks and Value Webs in Economic Integration of Digital Products

Rolf T. Wigand⁶²⁶

Overview and Underlying Premise: The underlying premise for this chapter is that a solution for DRM protection and related issues must be found on the business side, i.e. the solution must present itself within a business model, as technical solutions will always be temporary *ad infinitum*, resulting in endless revisions, upgrades, catch-up efforts, and improvements. There is no question that evolving and future distribution systems for images, music and movies will be digital and the distribution itself will be electronic via networks and e-channels. This contribution explores this setting in terms of economic and organizational underpinnings of electronic markets, networks and channels. We can presently observe the evolution of value networks, value-adding channels, as well as entire value webs in the distribution (and value) chain. A value web is a customer-driven network of independent firms who use information technology to coordinate their value chains to collectively produce a product or service for a market. Finally, we address some of these observations, descriptions and discussions in the context of DRM, specifically the music and movie industry. We will offer some insights, address current developments, but also some speculations how these industries may (and quite possibly must) progress.

I Introduction

There is little disagreement in most quarters of the information and entertainment industries that the future distribution of information, images, music and movies will be digital. Moreover, the distribution of such digital products will occur via networks and electronic channels. We need to explore the needed and appropriate organizational forms and market structure that make such distribution possible. In doing so, we will address electronic commerce, electronic markets, networks and channels. At the same time we need to realize that such distribution occurs along a value chains in value-adding networks and value-webs.

Newer information and communication technologies (ICT) enable organizational and business processes and are essential tools to create competitive advantage. ICT play an essential role in utilizing markets as a coordination form when conducting business⁶²⁷. They make personalization and mass customization possible⁶²⁸. The drivers, nature and magnitudes of these developments are the focal points and enablers of electronic commerce (EC). The widespread use of personal computers, together with the proliferation of telecommunications services and networks, the Internet and the WWW, as well as their joint integration, have made EC a reality, even for common citizens. It is in this context that we must

⁶²⁶ University of Arkansas at Little Rock.

⁶²⁷ See: Wigand, Picot, Reichwald (1997); Picot, Reichwald, Wigand (2003).

⁶²⁸ See: Wigand (1997b).

find suitable business models and solutions for the sale and delivery of digital products.

The bandwidth of EC spans from electronic markets to electronic hierarchies and also includes electronically supported entrepreneurial networks and cooperative arrangements. Market coordination mechanisms are their common characteristic. Services within the finance, tourism, brokerage or insurance industries, but also logistics and customer relationship management are typical fields of application. Delineating among differing forms of electronic markets becomes even more difficult, as:

- Organizational boundaries become fuzzy, change or disappear and, as market coordination forms, may also find a place within organizations themselves.
- Value-added chains change or entirely new ones appear, and value-added activities are newly distributed.
- Suppliers and customers become part of the value-added chain.
- Entirely new players become entrepreneurs who would not have entered a market prior to these EC developments.
- Disintermediation and reintermediation is frequent, but often the reintermediaries are different players.

The development of the Internet, as well as its special application, the WWW, demonstrates business' and industry's increasing interest in and recognition of the importance of EC⁶²⁹. With the advent of the Internet and WWW, a new medium has emerged whose potential is more dynamic than color printing, radio or television. The appeal of universal connectivity and access is driving firms and individuals to the Internet. Various developments over the last few years seem to suggest the Internet is *the* universal dial tone for conducting business, including the buy side (suppliers and logistics), as well as the sell side (customers). The aim of most EC efforts is to conduct business electronically with millions of firms of all sizes and millions of customers as well. The WWW has become a focal part of many firms' long-range strategic plans. The Internet phenomenon has indeed become a paradigm shift governing both businesses and consumers.

It may take time and considerable investments, but most observers agree various ICT enabled via the Internet will one day be a two-way window to the world through which we tweak our bank accounts, order office supplies, groceries and books or receive electronic entertainment (such as music and movies) on demand. Most of these things are already possible today, may even exist partially, even though they may not be retrievable yet in a very user-friendly fashion⁶³⁰.

I.1 Electronic Markets

One particularly intriguing application of EC is electronic markets. Markets are places of exchange where supply and demand meet. At the same time, markets are comprised of people or firms making judgments about values of objects and services. Value depends on individuals' or firms' desires in that the more they

⁶²⁹ See: Wigand (1995a/b).

⁶³⁰ See, e.g.: Benjamin, Wigand (1995).

esteem an object or service and are at the same time willing to trade for it, the more the object or service is worth. This in essence is the very basis of free-market capitalism.

A market is conceived to consist of goal-seeking firms, government agencies, or individuals producing some commodity or service, as well as all firms, government agencies and individuals purchasing the commodity or service. Within this market, the exchange of goods and services takes place. When the market is competitive, it is characterized by (1) many buyers and sellers, (2) homogeneous products, (3) easy entrance to and departure from the market, (4) low switching costs for consumers who wish to choose among suitable goods from competing firms, and (5) the availability of perfect information. Information is an essential ingredient for the functioning of any market and is exchanged frequently among buyers and sellers such as when product and price information is exchanged. *Perfect information* denotes that consumers will have all the information, i.e. complete information, (e.g., through advertising, news media, personal inquiry) they need to make informed, rational decisions about which goods and services to purchase in the marketplace. Often it would be a massive or highly cumbersome task to acquire perfect information and decision-makers may decide that they have sufficient or “good enough” information to make a decision, i.e. they then possess *satisfied information*.

One must make, however, a distinction between markets for information and a market for ordinary commodities on at least two counts⁶³¹. On the surface, information can be considered a factor of production. Another perspective enters the picture when information itself (such as with digital products) becomes a commodity and when private markets have formed in which information can be bought and sold as a commodity. Information then takes on a complex role as information has peculiar characteristics in that it is easily copied, transmitted, sold without destroying it, and that it is expandable, diffusive, compressible, difficult to establish property rights for at times, and sometimes it is a public good⁶³². The value of information is heavily dependent on the context of its use. Indirectly then, information may be defined by a description of its properties (most of these apply directly to digital products just the same):

- Information is an *immaterial good* that does not wear out by use.
- *Distribution* of information can either be done by the transfer on a material storage medium or by transmission over communication networks.
- Compared to physical products, information can be *duplicated and circulated easily*.
- The production of information usually causes *high fixed costs* for the first “copy” of the information and small or even vanishing marginal costs for every additional copy over a wide range of outputs. Nevertheless, information is not a free good, but a *scarce resource*.
- Information is *indivisible* and useful only in integer amounts.

⁶³¹ See: Ciborra (1993): 103.

⁶³² Cf., e.g.: Wigand, Picot, Reichwald (1997); Ciborra (1993); Wigand (1988b).

- Information *requires no exclusivity* of use.
- *The disclosure problem*: The use of information by one individual may reveal the information to others. Consequently, the information is shared in its entirety and unaltered, something that is impossible for physical goods.
- Information can be exchanged and traded as an economic *commodity*.
- Information is *not exclusively transferable*. If the property rights are transformed between producer and user, usually only a copy of the information is sold and the original information can still be kept at the producer.
- Information *cannot be inspected without being revealed*. The true value of information cannot be predicted *ex ante*, which is usually referred to as the *fundamental paradox of information*⁶³³.
- The *value* of information is closely connected to the user, i.e. it is only of value for the user if it enables him or her to improve decisions or productive activities.
- Information has a *life cycle* from production over dissemination to its terminal use. *Decay* and *lifetime* of information are highly dependent on the type of information.

What then are electronic markets? Electronic markets emerge through the automated mediation of market transactions. Consequently, traditional industry chains lose their relative importance since business can be conducted quicker and often with an increased number of opportunities. Electronic markets are abstract places where (1) exchanges (trade) occur, (2) where complete (*satisfied*) information can be found and (3) transaction costs approach zero. The market is viewed aside from the hierarchy as the second basic form of market coordination⁶³⁴. Between the two poles of “market” and “hierarchy” one may recognize a continuum of hybrid organizational forms⁶³⁵ that offer—depending on differing tasks situations—varying degrees of efficiency and, in turn, advantages. Based on efficiency reasons, the coordination form of the market lends itself well to standardized transactions of performance relationships that have little variability and are easily describable⁶³⁶. *Electronic markets*, therefore, are one selected institutional and technical platform for electronic commerce. Conceptually and technically, in principle, digital products lend themselves very well to be sold via electronic markets.

An electronic market then is a coordination systems characterized as follows:

- Coordination mechanisms are electronically supported ranging from simple support (e.g., price information) to complete electronic coordination (e.g., price formation).
- The deployment of information and communication systems simplifies information supply and evaluation activities.
- Information and communication technologies reduce increasingly the importance of time differences and geographic distances.

⁶³³ See: Arrow (1962).

⁶³⁴ See: Coase (1937); Williamson (1975/1981a/1981b/1985).

⁶³⁵ E.g., clan and strategic network; see: Wigand, Picot, Reichwald (1997).

⁶³⁶ See: Wigand, Picot, Reichwald (1997).

- Aside from equal opportunities as a market participant and the freedom of participation in that market, it is especially the openness to access the market that constitutes an elementary prerequisite for electronic markets.
- A fundamental characteristic of electronic markets is the participation of human actors and, therefore, the human influencing of market events through their expectations, experiences and the interpretation of market information. Fully automatized processes are, therefore, not electronic markets⁶³⁷.

I.2 Effects of Information and Communication Technology

Information and communication technologies are essential for a modern firm's optimal performance today, as they augment the firm's capabilities to coordinate business transactions within the firm, but also among firms such as between buyers and suppliers. In this context, Malone et al.⁶³⁸ identified three effects of information technology, to which Wigand⁶³⁹ added a fourth one. All four effects may lead to reduced transaction and coordination costs:

1. *The communication effect* — Advances in information and communication technology allow for more information to be communicated in the same time unit of time, thus reducing transaction costs⁶⁴⁰.
2. *The electronic integration effect* — A tighter electronic linkage between buyer and seller is enabled⁶⁴⁰.
3. *The electronic brokerage effect* — An electronic marketplace where buyers and sellers come together to compare offerings⁶⁴⁰.
4. *The electronic strategic networking effect* — Information and communication technology (including networks) enable the design and deliberate strategic deployment of linkages and networks among cooperating firms intended to achieve joint, strategic goals which, in turn, enable competitive advantage [such as in peer-to-peer networking and file-sharing with digital products]⁶⁴¹.

I.3 From Mediation to Disintermediation and Reintermediation

It is getting more and more complicated to clearly delineate the boundaries of today's firms due to their tight linkages and integration with other firms. In an economy based on the division of labor, trade has the task to compensate spatial, temporal, quantitative and qualitative tensions between processes of production and consumption. Driven by information and communication technologies' ability to produce even cheaper unit costs of coordination and transaction, firms have implemented new links for relating to each other. Geographic distance is often of little concern as modern telecommunication technologies perform at

⁶³⁷ See: Wigand (1997a/b).

⁶³⁸ See: Malone et al. (1987).

⁶³⁹ See: Wigand (1996).

⁶⁴⁰ See: Malone et al. (1987).

⁶⁴¹ See: Wigand (1996/1997b/2000).

very high speeds. An average credit card transaction takes about 4.5 seconds to secure an approval confirmation for the merchant. During the holidays when many gifts are being purchased and credit card companies' mainframe computers are overburdened, these companies lease computers wherever leasing is the cheapest (typically in India). The credit card transaction process between India and the North American location takes merely one second longer. Distance then does not appear to be a major hurdle in such transactions. Tight links among firms take many forms, such as electronic data integration (EDI), just-in-time manufacturing, electronic hierarchies and markets, strategic alliances, networked and virtual organizations, and others. The resulting new organizational forms indicate an ongoing transformation of value chains⁶⁴².

Intermediation is the bridging of incompatibilities between two (market) sides involved in a transaction. An intermediary then is an independent, profit-maximizing economic agent mediating between two market sides. Intermediaries are specialists in performing transactions, and the source of their efficiency is a reduction in the costs of these transactions compared to transactions without an intermediary. Mediation or intermediation has an important efficiency feature in all forms of trade within an economy. The resulting effect has been labeled the Baligh-Richartz effect and is demonstrated in Figure 1.

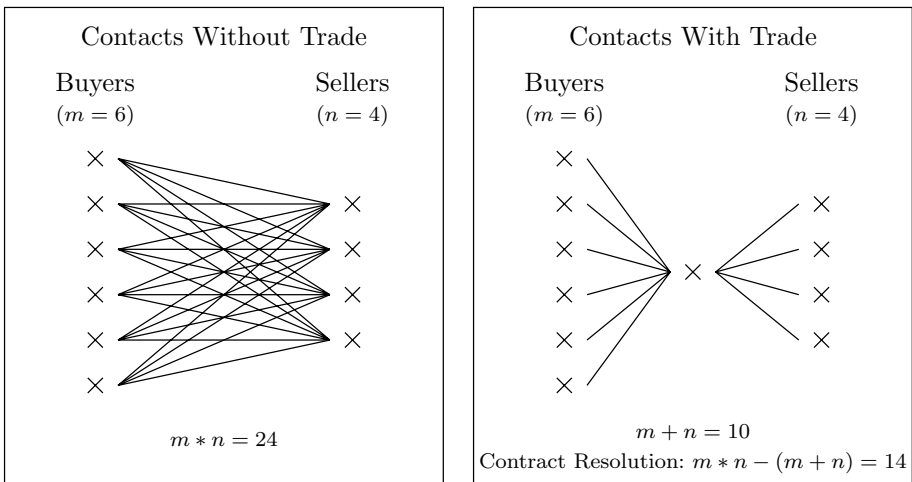


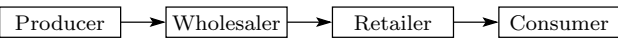


Fig. 1. The Reduction of Necessary Contacts through Intermediation

In a market with 6 buyers and four sellers a total of 24 contacts are necessary to get complete information. In contrast in the same market with an intermediary (or trader/market maker) great efficiencies are achieved due to this intermediary in that merely 10 contacts are necessary, a savings of 14. Figure 2 also illustrates that any sort of trade would be very costly and cumbersome without the intermediary. Moreover, market hierarchies that depend on intermediaries (e.g., the value chain from manufacturer, to wholesaler, to retailer and buyer) remain

⁶⁴² See: Benjamin, Wigand (1995); Wigand et al. (1997).

defunct if one in this chain drops out. Consequently, reintermediation becomes necessary or nothing happens at all. In general, reintermediaries search for opportunities in supply chains by breaking apart existing relationships into logical components and re-shuffling them to enable more efficiency, choice, or speed.

Playing Electronic Market Leapfrog

		Cost per Shirt	Percent Savings
A. Three Variants of Alternate Value Added Chains			
1.		\$ 52.72	0 %
2.		\$ 41.34	28 %
3.		\$ 20.45	62 %

B. Growth in Value Added and Selling Price

	Producer	Wholesaler	Retailer	Consumer ⁶⁴³
Value Added	\$ 20.45	\$ 11.36	\$ 20.91	
Selling Price	\$ 20.45	\$ 31.81	\$ 52.72	\$ 52.72

Fig. 2. Reconfiguring Industry Value Added Chains

Traditionally such linkages among firms were enabled through the mediating roles of wholesalers, retailers, agents, distributors, brokers, warehousemen, forwarders and “jobbers”. Today examples abound in which these mediating roles have been leap-frogged, replaced or eliminated. Benjamin and Wigand⁶⁴⁴ (see Figure 2) were the first to demonstrate such an example in conjunction with a high-quality shirt acquired in three variants of value chains within the shirt industry. Numerous other examples can be mentioned: brokerage firms, travel agencies, insurance agencies, grocery delivery services, as well as real estate agents⁶⁴⁵. Similarly, one may refer to leap-frogging (disintermediation) of traditional brick and mortar CD or record stores when buyers decide to buy their music directly from web-based CD outlets.

These developments have been labeled *disintermediation*. Disintermediation is the displacement or elimination of market intermediaries, enabling trade with buyers and sellers without the middle person. Often suppliers and their customers are linked directly today without any intermediaries. Previous intermediary roles, sometimes called middle professions, of brokers, agents, etc. between manufacturers and buyer/consumer may be replaced by an electronic market maker or by value networks (e.g., common carriers, on-line market places), which, in turn, enable *reintermediation*. In that sense one might argue that the middle person is not dead, as was predicted in the early days of EC, yet one

⁶⁴³ Consumer Transaction costs are not considered.

⁶⁴⁴ See: Benjamin, Wigand (1995): 67.

⁶⁴⁵ See: Crowston, Wigand (1999).

must realized that these reintermediaries are often very different players than the original intermediators.

Electronic markets allow firms to reach potentially very large customer groups at relatively low costs⁶⁴⁶. Additional discussion on market hierarchies will be found in the section on transaction costs theory. Value chains have been viewed traditionally as a linear, step-wise and linked phenomenon⁶⁴⁷. Rayport and Sviokla⁶⁴⁸, however, differentiate between the physical and virtual value chain and refer to the latter as *marketspace*. Today, it may make more sense to view virtual value chain as being linked to a matrix or web (the *Value Web*) that is accessible at each point and freely configurable.

A *Value Web* in this sense is a temporary web of independent companies, has no hierarchy, no vertical integration, and enjoys fluid, flexible, and dynamic relationships. An example is the electricity spot market where firms may purchase electricity 24 hours per day at the best price possible. Buying and selling in such a value web is dynamic and highly interactive. Within the DRM context, this concept applies as well: Value webs are also conceivable for digital goods when, e.g., a buyer enters a value web to find the best price, e.g., for a CD irregardless of the brand name of the supplier. The buyer enters the value web of his/her choice, searches, and buys the CD or movie of choice and leaves the web. The very same web constellation is available next time around when the need for another CD purchase arises. Japanese teenagers in large numbers bought music CDs on the web instead of from highly overpriced Japanese brick and mortar CD stores. The end effect, based on Japanese teenagers' buying behavior, was that CD prices in traditional Japanese CD shops were driven downwards drastically and stabilized at such lower levels.

A high degree of automated *interactivity* in EC transactions has always been a major goal to achieve. It appears also that the higher the degree of interactivity, the more perfected the electronic market might be. Nevertheless, one needs to consider the buyer's individual willingness and desire to be interactive in these settings. Many interactive services have been observed, ranging from online networks to two-way cable television to phone-based banking and investment services. Clearly, they have changed the way we inform, educate, work, play, manage our resources, and entertain ourselves. Such interactive services have changed fundamentally how businesses connect and interact with buyers and suppliers. Interactive services can personalize the information users need and use it in a manner suiting them best. Interactive services are usually easy-to-use telecommunications-based services designed for information exchange, communication, transactions and entertainment. Such services ought to encompass four essential features in order to ensure their acceptance: (1) The device or service must replace a process that is inefficient, costly or boring; (2) users must not be asked to choose between competing technologies; (3) users must not feel "tracked" or that their privacy seems threatened; and (4) users must perceive

⁶⁴⁶ See: Benjamin, Wigand (1995).

⁶⁴⁷ See e.g.: Porter (1985).

⁶⁴⁸ See: Rayport, Sviokla (1995).

that the use of the service (and information or communication technology) is relatively easy, user-friendly and non-complex.

The role of the market maker varies considerably with the various forms and types of electronic commerce. The market maker's most prominent role is evident when the market maker is the driver of the electronic market and can offer single-source channels, as is the case with teleshopping, electronic shopping, or the full-fledged EC setting through the use of an interactive website or set-top box.

I.4 Theoretical and Conceptual Approaches to Electronic Commerce

Seven theoretical approaches and orientations may be identified through which EC may be viewed: Transaction cost theory, intermediation theory, marketing, strategic networking, exchange theory, diffusion, and information retrieval. Given the present context, we will only focus on the first four theories, i.e. transaction cost theory, intermediation theory, marketing and strategic networking.

Transaction Cost Theory

Transaction Cost Theory is overall probably the most utilized theoretical underpinning for most forms of EC. Economists have classified transactions among and within organizations as those that (a) support coordination between buyers and sellers, i.e. market transactions, and those (b) supporting coordination within the firm. Figure 3 shows a typical hierarchy progressing from "manufacturer" to "wholesaler", "retailer" and "consumer" (or "buyer" in general). The associated respective transaction costs are depicted as well. Williamson⁶⁴⁹ points out that the choice of transaction depends on a number of factors, including asset specificity (CDs, e.g., have low asset specificity), the parties' interests in the transaction, and ambiguity and uncertainty in describing the transaction. Transactions may be broken down into production and coordination costs⁶⁵⁰. In this context, coordination costs include the transaction (governance) costs of the information processing necessary to coordinate the work of people and machines performing primary processes⁶⁵¹. Transaction costs may be viewed as the economic equivalent of friction in a physical system, i.e. if friction is too great, no or at least impeded movement will occur, suggesting that if transaction costs are high, no or little economic activity is likely to occur. Such transaction costs can be clustered into the following four types:

- *Search costs* — the costs of searching for products, sellers, and buyers
- *Contracting costs* — the cost of setting up and carrying out the contract
- *Monitoring costs* — the cost ensuring that the terms of the contract have been met

⁶⁴⁹ See: Williamson (1981b).

⁶⁵⁰ See, e.g.: Wigand, Picot, Reichwald (1997); Benjamin, Wigand (1995); Malone et al. (1987).

⁶⁵¹ See: Malone et al. (1987): 485.

- *Adaptation costs* — the cost incurred in making changes during the life of the contract

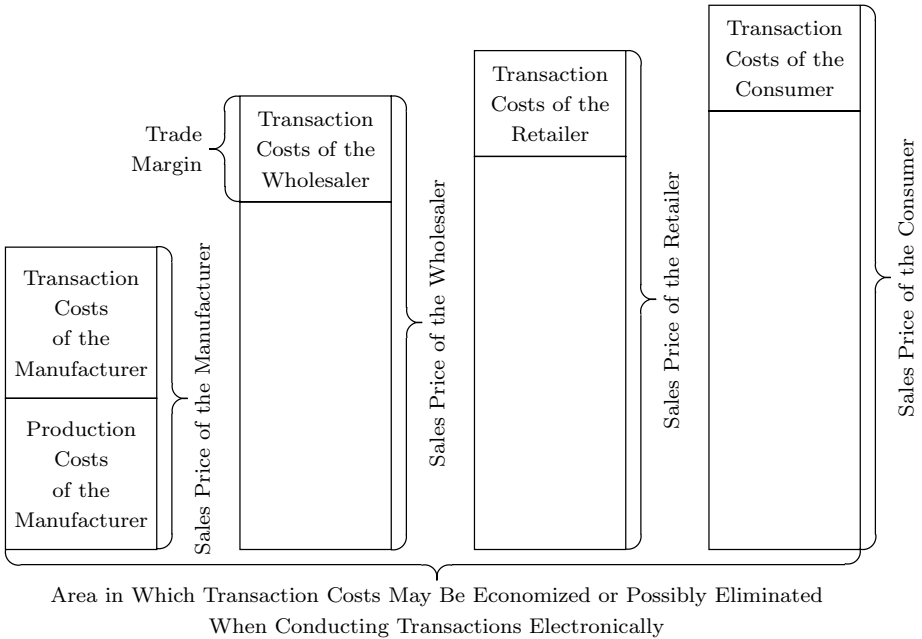


Fig. 3. Market Hierarchy and Transaction Costs in a Stepwise Fashion

As ICT continue their rapid cost performance Firms will choose transactions that economize on coordination costs. As ICT continues its rapid cost performance improvement, the unit cost of coordinating transactions will approach zero, thus enabling the design of innovative coordination transactions to fit new business needs⁶⁵². The ever increasing and innovative use of the WWW for the conduct of business are definite examples of firms' desires to economize on transaction costs. Figure 3 suggests that transaction cost savings may be achieved through the use of ICT within the entire market hierarchy and resulting market or industry value chain. Benjamin and Wigand⁶⁵² present an example of the purchase of a high-quality shirt with empirical cost figures clearly demonstrating actual savings in transaction costs resulting in considerable lower purchase costs for the consumer (buyer) (see figure 2). Moreover, this example demonstrated for the first time how the potential elimination of entire levels within the market hierarchy (e.g., wholesaler, retailer) may occur. This latter phenomenon of *dis-intermediation* is clearly observable in several markets and industry, as already referred to earlier. One may argue that with low-cost coordinative transactions, interconnected networks and their appropriate strategic deployment, and easily accessible databases, there would be a proportional shift of economic activity to low-cost electronic communications channels (especially the Internet and WWW) to conduct a firm's business.

⁶⁵² See: Benjamin, Wigand (1995).

Intermediation Theory

As our previous discussion already indicated, the notion of mediation, disintermediation and subsequent reintermediation plays a major role in the EC context. Successful as well as unsuccessful disintermediation and reintermediation efforts have shown that a large amount of up-front money is necessary and that a critical mass of users or customers needs to be built quickly. Moreover, it is self-evident that traditional or older middlepersons will tend to show strong resistance to any form of disintermediation. It is difficult and it takes time to develop and build domain expertise. Lastly, the economies of scale are in favor of the disintermediary in that acquiring a marginal new member can occur at a relatively small cost.

Minimally, intermediation is the bridging of incompatibilities between two (market) sides, recognizing that there are imperfections in a market. The actual intermediary then is an economic actor who is generally independent and operating on a for-profit basis. Intermediaries may be ordinary producing firms, located somewhere in the production chain and using a good together with other inputs to produce a “similar but different good”, or pure *middlemen* buying and selling the same good. In an economy based on the division of labor, intermediaries take on the task of overcoming spatial, temporal, quantitative and qualitative differences between processes of productions and consumption. Information intermediaries are unique and may be viewed as a special case in that their activities are information-based such as in information acquisition, processing and dissemination.

Three very basic theoretical approaches to intermediation explain and justify the existence of trade and, therefore, the existence and income of intermediaries in trade by saving resources (in accordance with Rose⁶⁵³ and others):

*Ricardo*⁶⁵⁴ — *Comparative Advantages in Costs*: Countries A and B specialize in the production of two different goods a and b, respectively. The production of good a causes lower costs for country A than country B, which in turn specializes on the production of good b. Assuming both countries aim to consume both goods, it is advantageous for both countries to specialize on the production of one good and exchange an excess in production of the good for the other good not produced. Ignoring transaction and coordination costs for the moment, *it may be advantageous to introduce an intermediary, i.e. a third party specialized to exploit economies of scale in the process of exchange, if the costs of direct transactions between the trading partners are significantly high.*

*Edgeworth*⁶⁵⁵ — *Advantages in Utility (Pareto Efficiency)*: In an isolated exchange with only two trading partners an opposite valuation of the good to be exchanged must exist, i.e. the problem of the *double coincidence of wants*. In a market with multiple agents the probability of an exchange is

⁶⁵³ See: Rose (1999).

⁶⁵⁴ See: Ricardo (1817).

⁶⁵⁵ See: Edgeworth (1881).

increased because the probability for the existence of opposite valuations is higher. However, finding a trading partner causes search costs that can be reduced by the introduction of an intermediary coordinating the process of exchange between the traders in the market. *So one main justification for the existence of intermediaries is the process of exchange in the existence of market imperfections that can be overcome by these third-party agents.*

*Reduction in Transaction Costs*⁶⁵⁶: An additional reason for the efficiency of intermediaries in the exchange process is the reduction of transaction costs and the necessity of asset-specific investments (e.g., information technology, infrastructure) as a precondition for the execution of transactions.

Four intermediary models can be identified in conjunction with Rose⁶⁵⁷ and others:

- *Market-making models*: Intermediaries are independent agents, buying and selling in markets. Buyers and sellers express their valuation for particular objects traded on the market via bid and ask prices (market-making). Intermediaries *process* this information distributed on the market
- *Matching models*: Intermediaries perform the matching of opposite market sides in bilateral search markets in return for a fee (e.g., firms and workers search for each other; agents acting on these search markets serve as intermediaries).
- *Advertising models*: Information intermediaries mediate, i.e. forward, bundle and process, information from sellers to potential buyers, being an alternative model to the direct transfer of information from sellers to potential consumers in form of advertising messages.
- *Search models*: An “information intermediary” collects information, e.g., about the quality of products in stores offering these products and subsequently sells this information to consumers who would otherwise have to perform their own search costs.

Marketing

All marketing efforts are based on the premise that there is a specific consumer or buyer audience. Consumers or buyers are specific individuals or firms who have needs that can be filled by other firms operating within a specific market. The field of marketing identifies three main foci of orientation: customer orientation, product orientation and profit orientation. A customer orientation denotes (a) an attitude and a pattern of conduct, as well as (b) the extent to which a firm tries to determine what its customers want and then gives them what they want. A product orientation suggests the clear identification of products, services, and related activities that distinguish themselves by (a) high demand among customers and (b) high levels of profitability. The reader may insert the digital product of a music CD, e.g., into the three foci of marketing orientation

⁶⁵⁶ See: Coase (1937); Williamson (1986).

⁶⁵⁷ See: Rose (1999).

and derive at his/her own conclusions about buyers' and sellers' behavior in the music CD market.

The basic challenge faced by all firms, then, is to identify needs and provide linkages and relationships to customers. In order to maximize such linkages and relationships to customers, a firm needs to form hypotheses and understanding about present and potential customers, addressing such questions as:

- What affects customer behavior?
- Which channels (face-to-face, advertising, WWW, publications, etc.) reach customers and how well does each channel accomplish this?
- What is the degree or strength of need or desire for the product or service?
- What are the appropriate appeals (or arguments) to which customers are most responsive?
- What is the customers' responsiveness to different types of sales devices?
- Which distribution channels work best and are there conflicts among them?

After these questions have been answered, the marketing dimension entails five general activities:

1. Identifying and selecting the type of customer whom the firm chooses to cultivate and learning the firm's requirements.
2. Designing products, know-how, and services that the firm can bring to market in conformity with customer desires.
3. Persuading customers to acquire and adopt products, know-how and services.
4. Displaying, moving, and to some extent storing products, know-how, and services after they have been developed by the firm.
5. Identifying potential products and services and their applications.

By engaging in those five dimensions over a longer period of time, firms will unquestionably benefit from having a clear picture of their target customers. EC can provide a direct linkage, an electronic marketing and information channel, between these target customers and the firm. Considerable rethinking has occurred based on such a customer-centric perspective as it enables new forms of relationship marketing and customer relationship management (CRM). Some firms experience *channel conflict* when new EC channels, e.g., the WWW, create a conflict with traditional channels. Should a firm, e.g., sell its own products directly via a WWW site to its end-customers and thus would be directly competing with its distributors who also sell to the same customers? If the answer is yes, how will the distributor react? Should this direct selling occur at a lower price than distributors sell the product for?

The term *liquid marketing* suggests itself as a suitable and appropriate descriptor of this setting. It denotes the disintermediated, nearly frictionless, personalized, individually accessible, customer-centric, immediate, cooperative, dynamic, fluid, rapid, computer-to-computer or -person, online, and interactive nature of this new form of relationship marketing.

Moreover, the concept of liquid marketing is enabled by the Internet: it allows for customized, almost interpersonal-like interaction, if one uses the interac-

tive multimedia, cooperative and feedback capabilities of the WWW, coupled with, e.g., the application of such features as agents, avatars, network dynamic functions, cookies, cacheing and the customer's willingness to complete profile information forms. This implies also that the user will give up a portion of his/her privacy as a tradeoff for convenience. This potential for interactivity certainly makes the medium highly attractive as requests, requirements, etc. certainly can be customized. Truly dynamic webs are evolving, enabling virtual applications, logic applications, collaboration, interaction, dynamic transactions, and entertainment. Moreover, such interactivity, sometimes labeled *interactability*, makes possible the often missing feedback loop in this communication process. Feedback, in turn, allows one to shape and incrementally customize the very next step in the diffusion and communication process reflecting the target customer's needs. Such customization is almost impossible when viewing the diffusion process via traditional advertising as a communication channel. EC marketing strategies, just as traditional marketing strategies, demand that we attempt to bring in the buyers and hook them to products and services offered such that it is very difficult for customers to leave or switch, resulting in competitive advantage. One such effort with regard to portals has enjoyed some success in this direction. The ideal portal is a web site sought out by many users or customers that constitutes the ideal entry point to the web, but it is also the sticking point, i.e. its final destination. Some evaluations schemes have been developed that attempt to measure the *stickiness* of such portals. Such a web site offers most things sought out by the user or customer, i.e. there is no reason to leave this site and go somewhere else.

Strategic Networking

Networking, i.e. the deliberate design and deployment of networks enabling new organizational forms, includes all three of the preceding topics, without which networking could not take place. Networking in this sense goes beyond the traditional means of reaching the target customer. This importance was already demonstrated in an empirical National Science Foundation-funded study by Wigand within the microelectronic industry and the role of industry, government and universities⁶⁵⁸. Other authors⁶⁵⁹ have stressed the importance of strategic networks and collaboration. Wigand et al.⁶⁶⁰ emphasize *strategic networks* as a distinct organizational form, i.e. being separate from other organizational forms: *hierarchy*, *market*, and *clan*. Networks have been studied as social systems, organizations, individuals and groups, entire industries, and political and social communities⁶⁶¹. In the present context they can be seen as a specific organizational form designed for the purpose of carrying out economic activities between the organizational form of "market" and "hierarchy". Under particular conditions we can label networks strategic networks, as they reflect connotations of long-

⁶⁵⁸ See: Wigand, Frankwick (1989).

⁶⁵⁹ Including: Ciborra (1993); Jarillo (1993); Sydow (1993); Wigand (1996); Wigand, Picot, Reichwald (1997).

⁶⁶⁰ See: Wigand, Picot, Reichwald (1997).

⁶⁶¹ See: Wigand (1988a).

term, rational importance, being proactive, selectivity, complexity, intention and coherence⁶⁶², strategic networks are defined here as the long-range, deliberate, cooperative, and goal-oriented organizational forms among distinct but related organizations that enable such network member organizations to gain or sustain competitive advantage vis-à-vis competitors outside the network, by optimizing transaction costs and minimizing coordination costs. Trust is an essential element of strategic networks that developed often prior to the formation of such networks and must be viewed as an important mechanism lowering transaction costs. Ideally, all member organizations continue to add value over time through adaptation, novel applications, learning, sharing of feedback, etc., which, in turn, will determine the strategic network's ultimate success.

This approach enables interaction with customers and suppliers that is simultaneous, almost fluid, efficient, flexible, interactive, maybe collaborative, conducive to innovation, and adds value to processes and the firm. Electronic networking suggests the use of listservs, bulletin boards, direct electronic inquiries, transaction-capable and interactive websites, etc., but also the deployment of deliberately designed and dedicated strategic networks in their entirety.

I.5 Discussion

We stated initially that the underlying premise for this chapter is that a solution for DRM protection and related issues must be found on the business side, i.e. the solution must present itself within a business model, as technical solutions will always be temporary *ad infinitum*, resulting in endless revisions, upgrades, catch-up efforts, and improvements. According to some accounts, some 50 million Americans alone are estimated to have illegally downloaded digital music in 2002. Eventually, this approach will essentially require that the music industry deputizes half the population helping to catch electronic pirates. After all, there are many (too many) people to sue. There is no question that evolving and future distribution systems for images, music and movies will be digital and the distribution itself will be electronic via networks and e-channels. We explored this setting in terms of economic and organizational underpinnings of electronic markets, networks and channels. We observed the evolution of value networks, value-adding channels, as well as entire value webs in the distribution (and value) chain. Following we will address some of the above observations, descriptions and discussions in the context of DRM, specifically the music and movie industry. We will offer some insights, address current developments, but also some speculations how these industries may (or must) progress.

With the advent of the Internet, a new distribution channel for music was provided utilizing MP3 and similar digital technologies. These, in turn, triggered novel forms of *sharing* music (peer-to-peer file sharing, sometimes also referred to as the *darknet*) that created a considerable legal and economic shakeup at the crossroads of content and technology within the music industry. The darknet is

⁶⁶² See: Sydow (1993): 80–81. In accordance with: Jarillo (1988): 32; Jarillo (1993): 140; Sydow (1993): 81, 82; Wigand (1996); Wigand, Picot, Reichwald (1997).

viewed as a collection of networks and technologies used to share digital content. In that context the darknet is not a distinct, separate network, but constitutes an application and protocol layer functioning within existing networks. Moreover, these developments also may be viewed as giant forms of communication networks and communities enabling this aforementioned *sharing* of music. The original focal facilitator of such networks was of course Napster and its 21 million users at its peak. Other forms of darknet creations include KaZaA, “Sneaker Net”, Morpheus, Grokster, as well as Gnutella. Darknets are generally highly efficient as they reduce distribution costs enormously — from an architectural, but also economic perspective — and they tend to promote new distribution methods and business creation.

Such file-sharing websites facilitate the sharing of copyrighted music MP3 files over the Internet by providing a registry of recordings, but it is the users who digitize the music themselves, using cheap PCs and free software, and then share these files without any form of payment. Unquestionably, this is an illegal activity and generally the courts have supported this as well.

For the music industry, however, time appears to be running out. In February, 2003, the Recording Industry Association of America (RIAA) reported a 9% decline in CD shipments vs. February, 2002, and a 6.8% decline in sales for all of 2002. Predictions are that sales are likely to drop by ten percent over 2002 in 2003⁶⁶³. With declining figures like that, the key to getting the publishers on board may not be legislation but it becomes imperative to convince them that a huge potential audience exists for paid, legally distributed digital music and that music-downloading services (such as MusicNet, Pressplay, and also Music-Match) have arrived. The music industry so far has not yet figured out what customers really want when they buy music online. There are many corporate histories around demonstrating what happens when companies did not adapt to new technologies. It seems as if the industry is investing 90 percent of its efforts on suing people, developing protection technology, even technology that may hurt or damage a user’s software and hardware. The remaining percentage seems to be spent on developing new distribution methods and business models encouraging consumers to purchase instead of steal music. For this writer’s taste this relationship should be flipped around. Hopefully the major record labels and movie studios will not join this historic list of firms who suffered at the wrong point of time from myopia.

A breath of fresh air blew through the industry, when Apple’s iTunes Music Store was launched April 28, 2003 with 200,000 library tracks compiled from music giants BMG, EMI, Sony Music Entertainment, Universal and Warner⁶⁶⁴. iTunes applies a very simple and straight-forward business model: Each song downloaded costs \$ 0.99. Underlying this model is then is the apparent assumption that resulting purchasing behavior is viewed as “impulse buying”. Apple CEO Steve Jobs won licensing deals with all five major record labels to open the

⁶⁶³ See: Leonard (2003).

⁶⁶⁴ See: Healy (2003); Tam (2003).

online music outlet — a coup that other industry-backed, subscription-based online services obtained only recently after more than a year of stagnant sales. Federal Judge Stephen V. Wilson in Los Angeles, however, dealt the entertainment industry a stunning blow on April 25, 2003 (for details see below), and in doing so stealing Apple's thunder, by deciding unexpectedly that making unauthorized copies of songs and movies on file-sharing networks is illegal, but that StreamCast Networks, the company behind the Morpheus network, and Grokster, another file-sharing network, cannot be liable as they do not monitor or control their user's online behavior. All file-sharing services combined are said to attract 30 million users each month.

Apple Computer, Inc. said on May 5, 2003 it exceeded record industry expectations by selling more than one million songs since the launch of its online music store a week ago. 275,000 tracks were sold in the service's first 18 hours. This astonishing success seems to suggest that the Apple iTunes Music Store and its underlying format is one of the most consumer-friendly methods yet of buying songs electronically and legally. Unlike competitors, the Apple service has virtually no copy protection. Customers are permitted to keep the songs indefinitely, share them on up to three Macintosh computers and play them on any number of iPod portable music players. With this business model, no subscriptions are necessary and buyers can burn unlimited copies of the songs onto CDs. According to various accounts, more than half of the songs were purchased as albums. Moreover, Apple also sold 20,000 of the newest iPod models over the weekend and received more than 110,000 orders. In spite of this strong success, one should note that the service is presently only available to Apple computer users in the U. S. and thus limiting sales to just 2.3 percent of the computer market⁶⁶⁵ for now. PC-based users may expect a PC version in December 2003. With such success, can we expect Microsoft, AOL Time Warner, Hewlett Packard, Dell and others to be in hot pursuit soon?

Music publishers are required by law to grant so-called mechanical licenses to labels and others who want to sell music. Accordingly, songwriters are paid 8 cents for each track that is physically produced. For example, if the writer has 12 songs on a CD and one million disks are produced, the songwriter receives \$ 960,000. New digital services, typically charging subscribers \$ 10 a month, permit subscribers essentially to "rent" songs. Such a subscriber may download unlimited tracks to a PC hard drive, but as soon as the subscriber quits the service, the stored music disappears. Such restricted downloads are referred to as "tethered downloads" and, as a business model, they serve as the foundation of subscription services. This model is attractive in that this prevents subscribers from making an infinite number of perfect digital copies of CDs or uploading them to the Internet where they could be easily distributed via illegal darknet services.

There is a major dilemma, however, in that tethered downloads do not fit the industry's traditional definition of an 8-cents-a-strike copy. Moreover, some

⁶⁶⁵ See: Tam (2003).

publishers are questioning if the subscription company earns \$ 10 per month by offering a collection of the publisher's songs, why should the publisher get paid only once? Based on sheer economics, until independent publishers are assured that they can do business on the same terms in the digital world as they can do otherwise, they are unlikely to budge.

Some music publishers are willing to negotiate and have agreed that the compulsory "mechanical license" covers tethered downloads, too. In an October, 2001 agreement with the RIAA, publishers accepted a \$ 1 million payment up-front in exchange for a promise that the services would account and pay for use of the publishers' work when the Copyright Office ultimately sets a rate. This, however, is not likely to happen until the market may be considered as somewhat mature.

U.S. District Judge Marilyn Hall Patel ordered the shut down of Napster Inc.'s Internet clearinghouse in 2000, stating that the company that revolutionized music distribution was encouraging "wholesale infringing" against recording industry copyrights and would likely lose at trial. Judge Patel noted that 70 million people would be expected to be using Napster by year's end unless the service is halted. A federal judge in 2001 ruled that Napster had abetted copyright infringement, and it has been off line since.

The RIAA sued Napster in December 1999 and accused it of encouraging an unrestrained, illegal, online bazaar. The heavy metal band Metallica also sued, claiming more than 300,000 Napster users traded its songs online. In 2003 the RIAA served Verizon with a subpoena demanding that the service provider disclose the identity of a user who uploaded more than 600 songs while connected to Verizon's Internet service. Verizon protested, but a U. S. district court judge ruled in favor of the RIAA and ordered Verizon to reveal the individual's identity. Verizon asked for a stay of the judge's order, but the Justice Department filing said the subpoena was legal and that no First Amendment protection would be violated through the disclosure of the name. More recently, in April 2003 the RIAA legally cracked down on universities through which many students download files illegally. Moreover, symbolically four students were charged (among many thousands of illegal student users) for their illegal practices, including offering allegedly over one million copies of popular recordings⁶⁶⁶. The students settled their law suits by agreeing to stop operating networks that swap music and to pay \$ 12,000 to \$ 17,000 each.

On April 29, 2003 the RIAA, unable to sue file-sharing networks into submission, launched an effort sending intimidating messages to, actually warning, users of KaZaA and Grokster file-sharing networks. Such messages (e.g., "DON'T STEAL MUSIC") inform the user that they risk legal penalties and that they can be tracked easily. Tracking is made possible through intelligent agents (robots) that monitor traffic on the network. The robot takes snapshots of files being shared and records the user's IP address. This address can be used to identify the user's Internet service provider who, in turn, will be served a subpoena to access appropriate records identifying the user's home, dorm room or office

⁶⁶⁶ See: Berman, Mathews (2003); Harmon (2003).

location within a company. Moreover, they are warned that they may be sued for their behavior (presumably heavy users only). Even high-ranking record industry executives stated that if parents received subpoenas or if high school students were faced with being viewed as pirates by college admissions officers that this then, in turn, “begins to affect behavior.”

It appears that the RIAA believes that it won a significant victory when federal judge Patel issued an injunction shutting down the Napster website and it seems that for the industry the Wild West days are over. The ruling might hold also broad implications for movies, books and other intellectual property that could easily be zapped around the globe via the Internet. The average Hollywood movie — according to the Motion Picture Association of America (MPAA) — costs \$ 80 million to produce and market. The MPAA estimates that piracy robs American studios of more than \$ 8 billion annually, excluding potentially very sizable losses brought about by online file-sharing. Movie companies have joined recording companies to sue Scour Inc., a file-swapping program for movies, photos and songs.

A major blow, however, was experienced by the music and entertainment industries on April 25, 2003 by ruling unexpectedly that two major online networks letting users copy music and movies for free are not violating copyright laws. U. S. District Judge Stephen V. Wilson issued a 34 pages-long decision that making unauthorized copies of songs and movies on file-sharing networks is illegal, but that the companies behind the Morpheus and Grokster networks are not liable for their user’s piracy. Accordingly, Morpheus and Grokster do not monitor or control what people do on their networks which absolves them from liability. RIAA and MPAA executives state that the decision will be appealed.

To date, Napster and its music-sharing offspring have succeeded in providing Hollywood’s continued and biggest headache. But the headache has not stopped there: A number of new technologies are emerging that may trigger a mega-headache. Together they enable the storing of copyrighted programming into convenient files that are downloadable and sharable. New compression software permits the shrinking of digital files into smaller packages that are quickly distributed via networks. Next it is possible to store such smaller files (several shelves of movies) onto laptops and even handheld devices. Then there is digital recording (such as TiVo) which can be found in several devices and computers. Moreover, new wireless systems are emerging that can be established without too many complications in the home or on campus along which music and movies files may be exchanged about 50 times faster than through most broadband networks. These four technological developments when combined seem to create the aforementioned mega-headache for the music and movie industry. It seems that the Napsterization of music and movies will continue. As a reaction the industry has begun to build numerous security and protection mechanisms into networks and computers that would limit copying and transmitting copyrighted digital material.

There is no question that the underlying legal issues are complex and nested, but legal victories by the RIAA certainly would not mean that the battle against

Internet-delivered music has been won. It seems that if the industry would be smart it would join, find its proper place and become a player in this new and preferred delivery method for music for over 20 million users. The industry embracing the new distribution technologies and channels should create the flipside of the *darknet*, i.e. they ought to embrace and create the *brightnet* that is designed and conceived to its needs, but meeting consumer expectations as well. Especially young music consumers, who often justify their behavior by arguing that CD's are too expensive and that artists do not get the money anyway, may be more negatively inclined, if not even outright hostile toward the music industry than most. They tend to argue that record labels should accept the fact that the Internet has irrevocably changed the music distribution business and that the industry instead should offer new electronic services such as attractively priced subscription services and schemes, chat sessions with artists or early ticket sales for concerts, which they would be willing to pay for. Others, on the other hand, state they buy as many or more CDs as they ever did because they are able to sample music free and discover artists they like.

Ironically, music publishers follow the user behavior on popular darknet website quite closely exhibiting somewhat of an ostrich-like mentality. BigChampaign, a market research firm, tracks file-sharing sites and music publishers have discovered a silver-lining in music theft data. This company can capture a vast amount of raw user feedback by hanging out on the highways constituting the darknet or peer-to-peer networks. Publishers then buy such data to find out, if Eminem or the Dixie Chicks is hotter this week. Moreover, they may find out which single off Ja Rule's album may be the next runaway hit and if a little known artist is more popular than anticipated. BigChampaign can segment the data into geographic and demographic subsets. It is being said that most of the major labels use BigChampaign services with some spending millions per year, nearly no one admits to using these services.

Distributing intellectual property in a physical format is one thing; doing this in a digital world is different. It is the user's willingness to trade copyrighted material, not Napster's and others' willingness of facilitating file swapping that the RIAA should be worried about. Creating strategic alliances, acting collaboratively, forming joint ventures with online stakeholders and facing (or better embracing) this delivery method would make solid sense rather than going after Napster's and others' throat or becoming its enemy. The Internet is packed with Napster-like programs that are much tougher to monitor and to shut down legally. Programs such as Gnutella, AudioGnome, scour.com, Morpheus, KaZaA, Listen.com, Napagator, and others will continue to put pressure on the music industry. File-sharing on KaZaA was said to be 1,491 % higher in June 2002 than in June 2001, according to ComScore Media Metrix. Even easier, such services could be moved off shore to a country outside the legal reach of the industry. The industry's own and long-awaited plans for selling downloaded music may have to be modified to add Napster-like capabilities, possibly even all-you-can-eat subscription services. The RIAA should not assume that one court ruling

or, for that matter, many court rulings will reverse the tide of technology. New file-sharing services pop up as fast as old ones are shut down.

Few analysts would doubt that darknets and darknet-practices will continue. Unquestionably, they tend to provide low-cost and generally high-quality services to vast numbers of consumers. In that sense the darknet will continue to co-exist with legal commerce and applications. This, however, creates an intriguing dilemma from an economic theory and business strategy perspective. More specifically, as security and copy-protection methods (such as stronger DRM systems) increase, the more legal commerce sales should decrease, as such security and copy-protection methods create a disincentive for buyers. A freely available song as an MP3 file on a darknet is just as useful as one purchased legally. Moreover, the legally purchased song has less utility as it is likely to be securely DRM-wrapped and thus does not lend itself for sharing. Herein lies an intriguing paradox: A seller of music is likely to make more money when selling unprotected music than when selling protected music. In order to succeed and get out of this paradox, the seller of music must compete with the darknet, yet he/she has to compete on the darknet's own terms: low cost and convenience⁶⁶⁷.

The music industry so far has not yet figured out what customers really want when they buy music online. There are many corporate histories around demonstrating what happens when companies did not adapt to new technologies. It seems as if the industry is investing 90 percent of its efforts on suing people, sending out messages telling users "Do Not Steal", "freeze" practices (locking up computer systems), "silence" programs scanning hard drives and deleting pirated music (and sometimes other files too), "interdiction" programs attacking personal Internet connections while downloading or sharing pirated music, as well as developing various other protection technology, even technology that may hurt or damage a user's software and hardware. The remaining ten percent seem to be spent on developing new distribution methods and business models encouraging consumers to purchase instead of steal music. For this writer's taste, this relationship should be flipped around. Hopefully the major record labels and movie studios will not join this historic list of firms who suffered at the wrong point of time from myopia. The consequences are rather stark: The recording and motion picture industries have no choice, but to adapt to these developments or become corporate dinosaurs. At the same time one needs to realize that this dance around information technology, DRM issues, business models and consumer needs and behavior is by far from over.

⁶⁶⁷ See: Wigand (2000).

3.3 Creating a Framework for Business Models for Digital Content — Mobile Music as Case Study

*Willms Buhse*⁶⁶⁸, *Amélie Wetzel*⁶⁶⁹

Abstract: This article examines and categorizes potential business model scenarios for digital content. The digitalization of goods like music and other content types leads to market uncertainties. As a result, offering parties on the supply side may not be able to sufficiently privatize it. On the demand side, due to changing cost structures for digital goods, consumers may not be willing to pay directly for any such goods. Therefore, enterprises are forced to develop new business models to respond successfully to this new market situation.

Firstly, definitions of business models for digital content and its important role in the strategic context of companies are being defined and examined. Following, we will point out challenges resulting from selling digital content in the digital net-economy, using the example of mobile music.

Based on the above assumptions we will examine the market for mobile music and categorize four different types of viable business models. In the first type, mobile music is used to promote the traditional offline business. The second category proposes a model in which consumers are willing to pay for additional services to access mobile music. The third and fourth scenario significantly differ from the previous two, as music providers are considered to protect their content by using digital rights management technologies. While in the third scenario, consumers access content using subscription systems, in the last category, secure peer-to-peer technologies (super-distribution) enable consumers to share and recommend copy-protected songs. The paper concludes with an analysis about the success of business models for digital content.

I Introduction

Digitalization is the basis for new developments in information, communication and telecommunication processes. These effects influence more or less all input factors in the value chain. Digitalization enables companies to transform physical products into immaterial binary codes. A digital product version yields the chance to easily establish innovative product diversifications. Moreover, it significantly reduces the cost of production, duplication and distribution. For example, whereas the duplication and distribution cost of *Microsoft's* entire digital Encyclopedia Encarta amounts to approx. US\$ 1.50, the comparable print version for ca. US\$ 250 per hard copy.⁶⁷⁰ This new cost structure enhances the creation of specific value propositions to small customer groups that were previously unprofitable to market. Summing up, the competitive landscape is profoundly changing. Industrial structures and barriers to entry dissolve and give room to aggressive new market entrants.

⁶⁶⁸ Bertelsmann Digital World Services.

⁶⁶⁹ University of Munich.

⁶⁷⁰ See: Downes, Mui (1998): 51.

A further consequence of digitalization is a change in product characteristics: As products may be transformed into a stream of information, it is no longer essential to own the physical product, but it is of crucial importance to control access to the consumption of the particular product.⁶⁷¹

Intangible products have similar characteristics to public goods. The digitalization and the distribution via the Internet further strengthen these features. A digital replication is not only a simple copy of the original — it is a perfect clone of the original product⁶⁷² with hardly any rivalry when consuming these products. Therefore, legal and/or technical protection is necessary to limit free rider behavior and to inhibit illegal use of digital products.

Due to this changing competitive landscape in the digital content business, traditional strategic analysis tools “... *may be largely out of touch with the evolution of modern competition in a technology-driven, global world that has seen a huge and rapid level of change.*”⁶⁷³

The convergence of media, telecommunication and information technology sector further pressures companies to develop unique competences or to develop strategic networks. “*What business are you really in?*”⁶⁷⁴

This basic question about the core business can no longer be answered statically, but has to be viewed in a dynamic and fast changing context. Because of the dissolution of barriers-to-entry and the deconstruction of traditional value chains, it seems vitally crucial to the authors to manage the company based on a long-term profitable business model.

I.1 A Strategic Approach to Defining Business Models

*“Instead of talking in terms of strategy and competitive advantage dot-coms and other Internet players talk about “business models”. This seemingly innocuous shift in terminology speaks volumes. The definition of a business model is murky at best. Most often, it seems to refer to a loose conception of how a company does business and generates revenue is a far cry from creating economic value, and no business model can be evaluated independently of industry structure. The business model approach to management becomes an invitation for faulty thinking and self-delusion.”*⁶⁷⁵

This edgy quote of Porter reveals an ongoing lack of a common definition of the term “business model”. The analysis of recently published literature offers a broad variety of different definitions for “business model”. As a result, the term business model is often used but rarely understood.

⁶⁷¹ See: Rifkin (2000): 3.

⁶⁷² See: Schaefer (2000): 1.

⁶⁷³ See: Bettis (1998): 359.

⁶⁷⁴ See: Hagel, Singer (1999).

⁶⁷⁵ See: Porter (2001): 72.

At a first glance, a business model does not seem to differ much from what was formerly called a business idea or a business opportunity. Often, the term “business model” is simply used to describe unique aspects of business activities or corporate strategy, and how these are realized in Internet ventures. This has led to considerable confusion,⁶⁷⁶ since there is no common understanding of the constituting components of a business model. Initial classifications concentrated on how businesses are run and how profits are generated.⁶⁷⁷ These first attempts were narrow in scope in comparison to subsequent definitions of the term “business model”. Following a similar line of thought, *Mahadevan* describes a business model as “*a unique blend of three streams that are critical to the business. These include the value stream for the business partners and the buyers, the revenue stream, and the logistical stream.*”⁶⁷⁸

These different definitions all include aspects relating to corporate strategy. Hence, business models have become a subject of strategy analysis.

In terms of strategy analysis, a business model is a description of the strategy of a firm that is able to convince shareholders of different opinions to invest in that specific company.⁶⁷⁹ Thus, a business model describes how a company (or a network of companies) establishes its market approach and value proposition. A business model illustrates the market and customer interaction within the company. On the other side, strategy includes an analysis of competitive advantages, value creation, value sources as well as core competences of the company. Therefore, a business model has to provide decision criteria whether and how a company should use market mechanisms to create value. In his “*theory of the firm*” *Coase*⁶⁸⁰ answered this question by opting for the alternative with minimal transaction cost. As transaction cost can be hardly measured, this criteria appears to be hard to put in the context of economic reality. It appears to be more realistic to assess a company’s efficiency by considering the company’s mid- and long-term market performance and market acceptance of its value proposition. In this context, business models measure the economic efficiency of a company by its unique competitive advantage and its unique selling proposition. In this context, a business model is the mere essence of a “theory of a firm”.⁶⁸¹ A business model then translates into a strategic concept combining the resource-based view with a market-based approach.

Following this pattern, we define business models as a representation of a company’s strategy. In order to compare different business models, we set up a research framework to identify the strategy components contained in all theoretical approaches. In search for the minimum overlap, we performed a survey of

⁶⁷⁶ See: *Mahadevan* (2000): 56.

⁶⁷⁷ See: *Schlachter* (1995); *Fedwa* (1996).

⁶⁷⁸ See: *Mahadevan* (2000): 59; similar: *Krueger, Bach* (2001).

⁶⁷⁹ See: *zu Knyphausen-Aufseß, Meinhardt* (2002).

⁶⁸⁰ See: *Coase* (1937).

⁶⁸¹ See: *zu Knyphausen-Aufseß, Meinhardt* (2001): 64.

current publications regarding business models and identified three fundamental elements which constitute a company's business model:

1. Architectural configuration of the value chain and its activities.
2. Value proposition of the product and description of the company's network.
3. Description of specific modes in which a business model enables revenue generation.⁶⁸²

Following the value chain of an industry or enterprise these three constituting elements can be add to the demand or supply side. The description of value chain and the companies' network gives an insight of how companies try to match with the needs of the market and fulfill their value proposition. In contrast, revenue and cost description explain how companies can compose their offers in order to correspond to market demands.

After a brief outline of specific characteristics of digital content in — what we refer to as — the digital net economy, we will establish different categories of business models in this environment.

1.2 Digital Content in the Network Economy

Prior to specification of unique aspects of digital content, we want to provide a clear understanding of the term "digital content".

Digital content has the following list of characteristics:

- 1) *Digital content can be produced*, but the production process differs from the standard production process for physical goods.
- 2) *High production costs*. First copy costs are mostly very high compared to the reproduction costs. At the same time, distribution costs of digital content are very minimal.
- 3) *Hardly any signs of wear and tear*. Once information is digitally saved, it can then be used over and over again without any signs of wear and tear.
- 4) *Importance of credibility*. It is usually difficult to gain upfront experience with consumption of informational goods. Evidently this is a high buying risk for the consumer, whether the product features really match his expectations.
- 5) *No rivalry in consumption*. In contrast to physical products, more than one consumer without any interferences or difficulties can consume information goods.
- 6) *Cost for copy protection*. While the cost for digital distribution seem rather low, content providers are facing increasing costs due to piracy. These costs are either explicit costs related to measures against piracy such as spoofing in P2P networks or lost opportunity costs that result from decreased sales.

Especially referring to the last two points, similar characteristics between digital content and public goods become evident. The theory of public goods holds that goods have different characteristics whether or not there is rivalry or non-rivalry

⁶⁸² See: Amit, Zott (2000).

in using them. *Public goods* are *non-excludable* and *non-rivalries* in consumption, while private goods are sold to those who can afford to pay the market price. In the music market, broadcasting as a public good is used to promote songs, while CDs function as a container for music sold as private goods.⁶⁸³ These similarities between public goods and digital content are even accelerated by the economic environment of the net-economy.

The term *digital net-economy* refers to settings in which business transactions are conducted via open networks based on the fixed and wireless Internet infrastructure. The following aspects characterize the digital net-economy:

- high connectivity,
- a focus on transactions,
- the importance of information goods and networks, and
- high reach and richness of information.

“Reach” in this context refers to the number of products and people that can be quickly and cost-efficiently reached via the communication network. Markets in the digital net-economy have an exceptional reach because of the near lack of geographical boundaries. In the net-economy customers and suppliers have instant access across regional and national borders. In other words, the quality sign “made in” is replaced by “made by”. Several other characteristics of the net-economy challenge the conventional structure of industries. These include the ease of extending one’s product range to include complementary products, or the proliferation of innovative market exchange mechanisms (i.e. P2P sharing). Industry boundaries are thus easily crossed as value chains are being redefined. These characteristics of the net-economy challenge the conventional theories of how value is created, and hence require a careful analysis of value creation und entrepreneurial success.

As a result, the value creation for digital content is affected. Not the digital content is necessarily the good in shortage but the attention of its consumer. Some argue that consumers have a limited budget for their attention, hence a competition for this limited good, the consumer attention.⁶⁸⁴ For this reason content needs to be bundled and presented on places with high customer attention. As a result ISPs and other gatekeepers gain importance for marketing digital content.

Compared to traditional techniques of strategy analysis, not only core competencies but also and especially value creation, congruence of the offering with customer values — such as pricing, as well as internal and external costs structures. The here presented definition of business models offer the opportunity to factor these new trends into the process of digital content value creation in the net economy.

⁶⁸³ See: Tschmuck (2000).

⁶⁸⁴ See e.g.: Lanham (1994); Goldhaber (1997); Franck (1998).

II Categorization of Business Models for Digital Content

More than all other product types digital content is affected and influenced by the characteristics of the net economy. Thus digital content and especially online music has become the perfect case study for analyzing existing and up-coming challenges in this new developing environment. For this reason we will discuss in the next section possible categorizations of business models for online music.

The starting point for this analysis is the assumption that the basic principle of the net economy as an efficient allocation mechanism works. However, uncertainties on both the supply and demand sides of the electronic market lead to insufficiencies. Two significant consequences regarding the business models resulting from the virtualization of media include: revenues are likely to be affected by the different associated cost structures, and business models are likely to be impacted by copyright protection issues similar to those, which exist for the Internet. Therefore, the following question is being examined: What possible business models are available to entrepreneurs to overcome both supply side and demand side market uncertainties in order to expand the online music market?

In the next section of this article, we will discuss demand-side uncertainties related to cost structures and revenue models as well as supply-side uncertainties related to whether digital content is distributed as a public and/or a private good. This article then combines the identified demand and supply side uncertainties into a scenario matrix. Finally a case study about mobile music is provided for each of the resulting four categories.

II.1 Demand-Side: Cost Structure and Revenue Models

Above, digital content was characterized as having high fixed costs or first-copy costs but very low incremental costs⁶⁸⁵, e.g. in the case of the music industry, producing the master-copy is very expensive while production of additional copies can be accomplished at very low marginal costs.⁶⁸⁶ A study conducted in England, Germany, Italy and France by Doglio & Richeri⁶⁸⁷ found that in the music industry the first-copy cost amounts to an average of 21.1 percent and manufacturing costs amount to 8.5 percent. The highest per-unit cost is attributable to marketing and sales with 49.9 percent, and the remaining 20.5 percent is allocated to label costs and margin. Additional cost elements beyond manufacturing costs include: retail obsolesce, returns, physical distribution and transport. Costs for technology, bandwidth and customer service, etc. also have to be factored in. The benefits of distribution of digital content do not significantly change the per-unit cost at current volumes. It does however offer the possibility to distribute in much larger quantities than in the physical world.

⁶⁸⁵ See: Skiera (1999): 97.

⁶⁸⁶ See: Kelly (1998): 54.

⁶⁸⁷ See: Doglio, Richeri (1996).

In the literature, revenues are divided into two main categories: direct revenues, which result from the consumer, and indirect revenues, which come from associated products via public or private entities.⁶⁸⁸ While in the literature a separation between different revenue streams seems possible, in the business environment, a wide spectrum of combinations can be found just like a newspaper company might have revenue streams from advertising, subscription and selling alerts via Short Message Service (SMS) or individual articles.

II.2 Supply–Side: Public and Private Goods

As discussed above, digital content has some of the characteristics of public goods, which are accelerated by features of the net economy.

Burke has shown how technological developments in the past gave rise to changes in copyright.⁶⁸⁹ At the same time, music as a public good has always accounted for a significant share of the music consumption. Already in 1999, according to IFPI, about 1.9b units of illegal copies were found with a value of 4.1b US dollars leading to a hypothetical market share of 36 percent.⁶⁹⁰ On the Internet, piracy has become an even larger mass phenomenon due to the availability of perfect digital copies. With non-excludable digital content, end consumers become *free riders* that are not willing to pay the market price as long as it can be accessed for free.⁶⁹¹

Five major labels dominate the distribution of music — for these music labels, the economic value lies in their artist contracts and in exclusive distribution of their recordings, which enables promotional distribution channels like free TV or radio.⁶⁹² Statistically, infrequent consumption of music albums as private goods accounts for about one hour a day, with revenues of 68 US dollars per music listener per year. On the other hand, public broadcast amounts to frequent, but superficial consumption of three hours a day. This results in 58 US dollars per music listener per year in advertising revenues for the broadcast stations per year from which music labels receive a much smaller percentage as compared to album sales. As a result, the music industry shows high interest in privatizing music in order to generate higher revenues not only from traditional products, but also from the mobile market. Increasing piracy challenges the privatization of music, and as a result the music industry has started a number of legal, marketing, educational and technology initiatives. Law suits from the Recording Industry Association of America (RIAA) against MP3.com, Napster, Verizon and others in the U.S. demonstrate the music industry’s efforts to battle copyright infringement. Just like on the Internet, users might access Mobile Music via wireless large area networks (WLAN) at hot spots like Universities or Airports — so-called “Offshore–Web–Hosting” — also offered from companies like

⁶⁸⁸ See: Zerdick et al. (1999): 25f.

⁶⁸⁹ See: Burke (1996): 51.

⁶⁹⁰ See: IFPI (2000): 2.

⁶⁹¹ See: Heinrich (1994): 26.

⁶⁹² See: Thurow (1994): 81f.

HavenCo.Com or Offshore.com.ai. De-centrally organized peer-to-peer-systems like Gnutella and FreeNet might continue to operate despite law suits driving consumers to “underground” systems — also referred to as the “DarkNet”.⁶⁹³

From a technology point of view, standardization efforts such as the Secure Digital Music Initiative (SDMI) or the Open Mobile Alliance (OMA) were started in order to develop specifications that include DRM. Many doubt that the industry can successfully introduce security mechanisms that are unbreakable or that can at least raise a significant barrier against piracy without creating much higher costs.⁶⁹⁴ Many examples in other media industries, like the current DVD-protection scheme, have failed to develop secure protection mechanisms. Additionally, on today’s Internet, only a single copy (even by re-digitizing from analogue versions) made available might be sufficient to be globally distributed in a short period of time leading to a substantial loss of control by the owner.

II.3 Scenario Modeling

The goal of using scenarios in the context of this article is to categorize various business models according to several case studies involving new distribution mechanisms like file sharing or Superdistribution. As described in the previous sections, the virtualization of content has two significant consequences regarding business models: first, the cost structure for the delivery is structured differently and thereby revenues may be affected. Second, the protection of copyrights has become more difficult in today’s networks.

	Public Good	Private Good
Indirect Revenues	S1	S3
Direct Revenues	S2	S4

Hence, four scenarios can be deduced by combining these two uncertainties into a matrix that represents both supply and demand.⁶⁹⁵ In this article, for each of the scenarios, one case study is described and possible revenue models are given.

Assumptions

These four business model scenarios are subject to the following assumptions:

- In the mid- to long-term, no business models will be viable which infringe on copyright laws. However, there might be systems without commercial interest that face no legal consequences for enabling illegal copies. Open-source-file sharing systems belong in this category.
- Revenue models are based on rational entrepreneurial decisions. Artistic, voluntary or otherwise motivated scenarios are excluded.
- Most importantly, these scenarios anticipate a slow migration towards digital technologies, meaning that traditional media companies maintain distribution control over physical storage media like CDs and DVDs. Zerdick et al.

⁶⁹³ See: *Biddle, England, Peinado, Willman* within this book on page 344.

⁶⁹⁴ See: Albers, Clement, Skiera (1999): 83

⁶⁹⁵ See: Buhse (2003).

state that electronic markets do not lead to an immediate substitution of the existing value chain. Nevertheless, it is leading to a constant erosion of traditional value chains and the orientation towards the demand side.⁶⁹⁶

In conclusion, a world of digital content with or without DRM seems realistic and the scenarios will be able to describe both views.

In order to further analyze business models for digital content, as defined above the following steps will be taken:

- Pre-conditions for a successful market transition from the traditional to the digital environment;
- Harmonized interests of the value chain participants;
- Potential revenue sources for digital content;
- Categorization of business models that reflects content as public and private goods and creates a relationship to the revenue sources; and
- Findings and recommendations can then be deducted from those scenarios.

In order for the reader to understand its practical implications, in the following case study these steps are implemented for Mobile Music.

III Case Study: Scenarios for Mobile Music

Online distribution became an underground phenomenon from the inception of content downloads over the Internet.⁶⁹⁷ Preconditions for Mobile Music are increasingly positive, as all participants — both from a market and resource based view — in the mobile value chain seem to have interests in successful business models.

This case study starts with a brief analysis of the market pre-conditions: How Mobile Music can drive successful end consumer business models:

- Consumers are accustomed to Mobile Music (using walkman/portable CD/MP3 players). Additionally, listening is a key functionality of phones.
- Music consumers and wireless pioneers are congruent (under 25 years).
- Little input functionality for linear content is required (play, pause, fast-forward, etc.).
- Formats and rendering devices are already available.
- Content preparation efforts are limited to the extent that audio content is digitally available as compared to books and graphics, and therefore little conversion is required for music or audio books.

With billing systems integrated in handsets, security has to be higher as compared to PCs, so DRM might as well leverage the same secure infrastructure. Security has been a big issue on the Internet, for both the content owners and the consumers. In the wireless environment, especially on handsets, hacks are much more difficult. As Consumers trust their cell phones (irrespective of their provider) as their billing partner for calls. Billing for content will become much

⁶⁹⁶ See: Zerdick et al. (1999): 177.

⁶⁹⁷ See: Pettauer (2000).

more convenient and trustable for the consumer through these carriers or other trusted third parties with existing billing and trust relationships. Also, privacy and data protection on the consumer side seem to be perceived as less of an issue compared to the Internet, where consumers fear that personal and payment data might be accessible to unauthorized parties. At the same time, security implemented on Subscriber Identity Module (SIM) cards or on chips seems more secure than software implementations on an application or even system level.

Though much literature can be found prognosticating a significant change in the competitive environment of the music industry, little research exists on the combination of revenue models and property rights in the field of Mobile Music.⁶⁹⁸

III.1 Mobile Music Value Chain Participants

With growing bandwidth and increasing handset capabilities, premium content becomes accessible via mobile end devices just like on today's Internet via the PC.

Involved in the value chain of mobile content are mobile content owners or copyright holder, aggregators, carriers, handset manufacturers and consumers with joint interests in successful mobile content.⁶⁹⁹

Content Owners

Re-purposing existing content for the new mobile distribution channel can be a very profitable business due to little upfront investments required for content creation. Just as on the Internet, competing with piracy and illegal copies turned out to be a major challenge for those, which are involved in the digital content business. Mobile content owners can only earn back their investments in mobile content if their copyright and content are protected. Content owners are unlikely to allow premium content to be distributed without effective DRM, especially in Europe and in the U.S.

Aggregators

Aggregators draw traffic with attractive content and their own brand value. Aggregators may take any form in the wireless world: carriers, portals, device portals and Internet-based portals (e.g. Yahoo!). Revenues are generated mostly from commerce transactions and advertising. Aggregators face the same challenge as content owners: to control the distribution of mobile content without the risk of overwhelming piracy.

Carriers

Carriers (and mobile network operators) want to capitalize on their heavy investments by using their networks for services beyond providing bandwidth for voice. The re-use of billing capabilities and bandwidth for mobile content is ex-

⁶⁹⁸ See: Zerdick et al. (1999): 53.

⁶⁹⁹ See: Buhse (2002).

pected to drive profitability in the future. By providing unique, differentiated content, carriers can increase average revenue per user and significantly lower their churn rate.

Handset Manufacturers

In a market close to global maturation, handsets can be differentiated by providing more functionality that the consumer would be willing to pay (instead of the provider subsidizing it). At the same time, handset manufacturers, just as carriers, have to increase their brand loyalty by providing attractive services and applications to consumers. In order to compete with rising “no-name” manufacturers, established brands have started to provide content through their online-clubs and -portals.

Consumers

The consumption of mobile content has always been an attractive proposition to consumers and is deeply interwoven with today’s media consumption behavior (books, newspapers, walkmans are just a few examples). Increasingly, consumers are demanding content be transferable across multiple (mobile) devices.

III.2 Potential Revenue Sources for Mobile Music

Additionally, a number of different revenue models for Mobile Music are possible.⁷⁰⁰

- *Airtime sharing* refers to the participation of content suppliers in connection revenues (per time unit or per data packet). To a great extent, the size of the connection revenues generated with attractive mobile content will determine the near-future success of mobile telecommunications firms. However, the extent of content suppliers’ participation in revenues will vary widely (between 0.50 percent and 10 percent).
- *Promotions and Sponsorships*: The mobile phone can deliver highly effective and targeted marketing messages. Mobile music can even include marketing or advertising messages, like a jingle or additional information (“The album is released on December 6th”), and can link directly to a purchase portal that allows the user to buy more.
- *Transaction-oriented revenues* will play a key role in the mobile environment enabling content providers and aggregators to recoup their investments. Commission rates will vary between 2 and 15 percent, depending on the content vertical (e.g. for entertainment offerings, 7–9 percent). At the same time, content can be forwarded to other consumers with specific restrictions attached (in DRM terminology, this is referred to as “Superdistribution”).
- *Content aggregation and subscription* describe the sale of content to consumers based on a flat periodic fee for unlimited (or capped) consumption. Content can either be generated specifically for the purpose, or comprise a

⁷⁰⁰ See: Buhse (2002).

selection of previously existing content that is otherwise sold unbundled. Mobile content subscriptions can be sold with the provider contract at sign-up (e.g. 40 Euros for 2,000 minutes plus three free subscriptions).

- *Levies or taxation on devices or bandwidth:* In some countries in the EU, like Germany or France, copyright levies are applied e.g. to blank media, recording equipment or special ICT devices. The same could apply to handsets or mobile memory such as SD cards. Collecting Societies or (other) clearing-houses would then remunerate the collected levies to the copyright holder. It is important to note that today, levies are meant as a compensation for copyright exemptions like the most important one, the private copies. This is not equal to copies distributed over digital networks.

III.3 Four Business Model Scenarios

In the following, the mentioned above scenario matrix is applied to Mobile Music with the four scenarios Filesharing and Beaming, Music Service Providing, Combined Subscriptions and Superdistribution (MMS).⁷⁰¹

	Public Good	Private Good
Indirect Revenues	Filesharing and Beaming	Combined Subscriptions
Direct Revenues	Music Service Providing	Superdistribution (MMS)

Tab. 1. Scenario Matrix for Mobile Music

First Scenario: Free Peer-to-Peer Distribution

In less than two years Napster became the largest music library in the world with about 1b titles. Napster was not engaged in economic incentive or marketing activities. Even more importantly was, that the music industry was not involved.⁷⁰² At a very high level, file sharing systems or peer-to-peer-networks (P2P) aggregate and distribute information. With either central or de-central listings, files be can searched for, transferred and stored locally. The main challenge for content owners was Napster’s mass phenomena. Since its launch, Napster attracted almost 70 Million users who knowingly violate copyright laws.

The purpose of open-source-file-sharing systems is to freely distribute information beyond any control and commercial interest (e.g., Gnutella developed by Gene Kan and FreeNet designed by Ian Clarke are examples). Gnutella and FreeNet are designed to run de-centralized — just like beaming content between handsets — which makes it almost impossible to control or to shut down. As a result, not only music files, but also illegal content such as child pornography and terrorist instructions can be found — just like a “digital black market”. The main challenge of these systems is that they can only scale with resources such as content, bandwidth and storage from their users. Because this content can be viewed as public goods, these systems attract *free riders* — people unwilling to give any contribution in return. During a study of the Gnutella Network it was

⁷⁰¹ See: Buhse (2002).

⁷⁰² See: Becker, Ziegler (2000): 14.

found that 70 percent of the users do not give any contribution to the system, and that half of the searches were answered by just one percent of the participants. Apart from a significant loss of system performance with longer search and download times, it increases the system's vulnerability as the system may collapse with the shut down of this one percent of peers. On the other hand, there are concepts like *seti@home* with users voluntarily contributing resources in exchange for prestige and reputation. As a result, file-sharing systems seem to be able to overcome today's challenges and will play an important role in the distribution of Mobile Music.

How can the music industry embrace such systems to generate revenues? Revenues can be generated indirectly from Mobile Music in return for the value of consumer's attention.⁷⁰³ This attention can be used to promote either the physical album or the artist in order to increase popularity and thereby earn higher merchandising and advertising revenue as well as from live events. As a result, with Mobile Music being a public good in this scenario, the combination of online and offline business by integrating Mobile Music and traditional marketing and distribution seems a profitable business model. Despite legal battles from the RIAA arguing that illegal copies cannibalize album sales, market studies are inconclusive at this point. Jupiter identified Napster usage as one of the most important factors for increased music purchases.⁷⁰⁴ On the other hand, album sales were decreasing in record stores close to universities where file sharing supposedly reached high usage among students.⁷⁰⁵ In 1999, Creed offered their hit song on 100 web sites for free downloads and in the process stimulated their album sales. Coincidentally their album "Human Clay" reached the top of the billboard charts.⁷⁰⁶

Nevertheless, substitution of the promoted traditional media like CDs and DVD-Audio might increase as soon as a comparably comfortable infrastructure for Mobile Music exists.

Second Scenario: Music Service Provider

Provided Mobile Music is a public good, collecting direct payments seems almost impossible unless the value lies primarily in the functionality and services rather than in the content itself.⁷⁰⁷ In this scenario, instead of copy protection, service-oriented new business models are developed to eliminate the motive to copy. Besides content, these services and applications offer convenience, reliability and fast access to music almost anywhere, anytime; these services are referred to as the *celestial jukebox*. This sector is expected to grow from 2.5m today to 12.3m in 2003 in the U.S.⁷⁰⁸ These revenues would come from charging the con-

⁷⁰³ See: Seidel (1993): 87.

⁷⁰⁴ See: Sinnreich (2000): 1.

⁷⁰⁵ See: VNU (2000): 2f.

⁷⁰⁶ See: Committee on Intellectual Property Rights and the Emerging Information Infrastructure (2000): 80f.

⁷⁰⁷ See: Deutsche Bank (2000): 14.

⁷⁰⁸ See: Black (2000).

sumer directly for the usage of these services and application fees and not based on the consumed content (an example would be monthly usage fees for a media play-back application). Ultimately, those companies — including the carriers — would have to combine content, community, application services, and context and search functionality. Personalization plays a crucial role in attracting consumers and providing lock-in.⁷⁰⁹ In the networked economy these versions and even individual products and services are achievable due to smaller transaction and production/service costs.⁷¹⁰ Using a feedback loop mechanism for Mobile Music, personal play lists can be generated, recommended, updated and shared among other users. Large description databases like Moodlogic or Gigabeat can analyze relationships among titles and artists according to rhythm, instruments, contextual information and even mood.

Third Scenario: Subscription Models

Protection technologies play an important role in determining whether a media product is a public or a private good. In scenarios three and four, Mobile Music is considered a private good as content owners are able to restrict access to the content, thereby introducing the possibility of excluding free riders and charging for their Mobile Music.

For subscription models, watermarking⁷¹¹ and fingerprinting⁷¹² can provide important contributions to the field of intellectual property protection within a more extensive security framework for identification and proof of ownership.⁷¹³ By embedding a watermark into the compressed audio signal during delivery, the customers are aware that a watermark may identify them.⁷¹⁴ Hence, users can be made responsible if the signal is found outside the legal domain by a trigger technology, even in a decompressed and analogue representation. In contrast to encryption technologies, watermarks and fingerprints could be used with today's infrastructure for CD-Audio as well as MP3-devices. Subscriptions bundle a large number of information goods for a fixed price and in a variety of circumstances a multi-product monopolist can extract substantially higher profits by offering one or more bundles of information goods than by offering the same goods separately.⁷¹⁵ At the same time, bundling can be used to introduce new artists and titles as a strategy to overcome the information paradox, which states that the value of information can't be determined *a priori* of consumption.

In this scenario, for the first time in their history, the music industry has the opportunity to create a continuous relationship with the end consumer. This relationship offers a foundation on which Mobile Music can generate substantial revenues. Revenues can be considered indirect when charged independently from

⁷⁰⁹ See: Heinrich (1999): 32.

⁷¹⁰ See: Piller (1998): 16.

⁷¹¹ See: *Petitcolas* within this book on page 81.

⁷¹² See: *Heere* within this book on page 93.

⁷¹³ See: Goldhammer, Zerdick (1999): 96.

⁷¹⁴ See: Tang (1998): 24.

⁷¹⁵ See: Bakos, Brynjolfsson (1999): 2f.

the usage (e.g. in combination with a carrier's monthly plan). Nevertheless, the subscription model represents a mix between indirect and direct revenues. Forrester expects additional revenues from subscriptions of 3.3b US dollars.⁷¹⁶ A premium membership might offer a flat rate, eventually combined with services from the second scenario, while an advertising-based membership might limit access in quantity, time or actuality.

III.4 Fourth Scenario: Superdistribution

- In 1990, a visionary architecture was developed for the distribution of digital goods. The Japanese Ryoichi Mori⁷¹⁷ coined the term *Superdistribution* for this new concept of licensing information. The fundamental idea is to allow free distribution of digital content, while controlling access to usage and changes with the content owner defining the terms.

After securely encrypting the music with a key, the package can be digitally delivered to the consumer's end device.⁷¹⁸ There, the locally installed trusted tool gains access to the digital content with an unlock key which leaves the file locally encrypted and streams the digital content into the memory for "on the fly" decryption. The user, who has agreed to the terms and conditions of use, now has the license to access the content. The usage is recorded and the transaction is reported to a clearinghouse to initiate payments and backup system information. Using the Superdistribution concept, consumers can recommend and share files among each other via email, MMS, physical media and other file sharing technologies. Still the copyright is being protected and the content owner maintains control and determines payment collection.

Under the third scenario bundling was mentioned as being attractive for content companies to extract higher profits. In the music industry this has always been the case with album sales where only one or two hits from an entire album initiate the purchase. Digital products possess optimal de-bundling capabilities, which in turn can be re-bundled for custom-mixes. With multimedia messaging and Superdistribution, consumers might start "cherry picking" their hits thereby endangering the traditional revenue model of album sales. In this scenario, by using DRM and Superdistribution, major labels maintain control over the distribution of music and might even be able to more effectively enforce their copyrights.

⁷¹⁶ See: Schreier (2000): 12.

⁷¹⁷ See: Mori (1990).

⁷¹⁸ See: Tang (1998): 23.

III.5 Case Study Conclusions

In this case study, scenarios for mobile business models that depend on uncertainties on the supply and demand sides of the music industry were examined. The following findings and recommendations can be deducted:

- Transaction revenues offer a preferable revenue option for Mobile Music as it is independent from bandwidth use, allowing for more flexible pricing schemes. Pricing that can be adjusted to consumer preferences, and not based on costs, has traditionally been higher for transactions (i.e. CDs) than based on advertising (i.e. Broadcast).
- In controlled environments like today's carrier networks, the privatization of Mobile Music seems likely with the adoption of DRM, as all value chain participants have a long-term interest in higher transaction revenues. This opens different revenue streams like subscription plans and Superdistribution for copy-protected music from scenarios three and four.
- In a less controlled environment with network access via WLAN to today's Internet, the adoption of DRM seems more difficult. Users still might be able to access pirated content — the “digital black market” — and thereby bypass the Mobile Music value chain. Revenues can only be generated as in scenario one and two, by promotions, sponsorships and the license of Mobile Music services mainly based on application fees.

In providing reliable access to illegal copies, piracy sites may still be accessible via WLAN. However, making payment mechanisms and customer service simultaneously available to thousands of people remains the more complex task. Which companies are able to position themselves in the role of music service providers?

- Companies with music brands emphasizing repeat visits such as those established by radio and television stations or music retailers; these companies have already proven their ability for selection and aggregation of music.
- Companies with strong existing customer relationships, through billing and access like the mobile carriers, might be able to benefit from their knowledge about their customers and provide better, personalized services based on consumer preferences and location.
- Companies with strong ties to end devices, like device-specific soft and hardware-developers as well as the manufacturers of consumer electronics themselves. These companies might be able to expand their revenues beyond hardware and offer services through the user interface that they control. A strong customer relationship via the end device will add service contracts to revenues from devices.

Under current copyright law, most companies might have to negotiate licenses directly with the music labels, their syndication partners or through royalty collecting entities in order to legally offer these services. This will enable the music industry to shift revenues from physical media to the mobile world.

IV Summary

This article is based on the assumption that business models are the new tool for analyzing economic success and value creation in the developing environment of the net-economy. For this purpose we started this article by defining and analyzing digital content and its challenges. It was shown that business models are an abstraction technique in reflecting the strategy of companies in the networked economy.

Scenarios for digital business models that depend on uncertainties on the supply and demand sides of the music industry were examined. It was argued that digital content could be a private good, through the usage of digital rights management, or a public good, due to insufficiencies in absolute content protection. It was also argued that the willingness of consumers to pay for digital goods may determine the nature of direct or indirect revenue streams. As a result, consistent business models in four scenarios were developed for the case study of Mobile Music, demonstrating that a spectrum of potential revenue streams exists for Mobile Music both as a public and private good. The main distinction between these scenarios depends on the supply side, where copyright can be protected by digital rights management technologies.

Business models can be categorized into a matrix by combining supply and demand side. Here digital right management contributes in providing alternatives for revenue generation by allowing the content provider to privatize digital content.

Companies will reach a competitive advantage if they evaluate their digital content offering by considering different business models scenarios and prioritize their positioning accordingly. The presented matrix enables companies to reach decisions in accepting their digital content offering as private and public good — in order to reflect the characteristics of digital content from a resource based perspective. On the other hand, companies can consider different revenue models for digital content — and thereby taking a market based view. Therefore DRM-systems seem to be the key requirement for successful business models and a source for competitive advantages.

It still may be too early to base further analysis on industry data like content revenues, so it becomes apparent that future research in this area is needed, especially in order to further analyze implications of the suggested scenarios from various perspectives, including market size and consumer benefits.

3.4 Impacts of DRM on Internet Based Innovation

*Arnold Picot, Marina Fiedler*⁷¹⁹

“[. . .] That ideas should freely spread from one to another over the globe, for the moral and mutual instruction of man, and improvement of his condition, seems to have been peculiarly and benevolently designed by nature, when she made them, like fire, expansible over all space, without lessening their density at any point, and like the air in which we breathe, move and have our physical being, incapable of confinement, or exclusive appropriation. Inventions then cannot, in nature, be a subject of property.”

Thomas Jefferson, 1813.

“With respect to a great number of inventions in the arts, an exclusive privilege is absolutely necessary in order that what is sown may be reaped. [. . .] He who has no hope that he shall reap, will not take the trouble to sow.”

Jeremy Bentham, 1843.

I Introduction: *Coase* Theorem and Its Impact on Internet Based Innovation

Neoclassic theory assumes that individuals solely strive for maximization of their utility function reflecting their respective preferences. Thus, decision makers will only consider costs and benefits which have an impact on their individual utility function. Therefore, if an individual's action affects the utility of another party without impact on one's own well-being, this impact will not be taken into account. Effects like this (i.e. positive and negative external effects or externalities) can not only prevent an economic agent from investing in such a good,⁷²⁰ but can also lead to over investment.⁷²¹ For example, in case of positive externalities, the profit seeking agent does not receive compensation for the benefits she bestows on other parties; therefore, she will not invest sufficiently into these activities. This may result in inefficient markets for this kind of goods.

To address this problem and motivate agents to innovate⁷²², most industrialized states grant exclusive exploitation rights like copyright or patent protection to an inventor.⁷²³ Thus, for a certain period of time, the inventor can gain monopoly rents from her invention.

⁷¹⁹ University of Munich. The authors would like to thank Dagmar Fiedler-Heer, Dr. Berthold Hass, Harris Hadjicharalambous and Egly Pantelakis.

⁷²⁰ See e.g.: Olson (1985); Hardin (1982); Ostrom (1990).

⁷²¹ See e.g.: Coase (1960).

⁷²² That is invention and exploitation of new goods and services; see: Roberts (1988).

⁷²³ See e.g.: Machlup, Penrose (1950): 11: “That a man has a ‘natural’ property right in his own ideas was a principle solemnly adopted by the French Constitutional Assembly in 1791. In the preamble of the patent law passed

Coase showed that in case of zero transaction costs, an efficient outcome will occur regardless of the initial assignment of property rights.⁷²⁴ The right will end up with the party who can achieve the largest output. If she does not receive the right directly from the legal or judicial authority, she will purchase it from the other party, who profits from selling it. Therefore, in a world with no transaction costs, any allocation of property rights is equally good, because inefficient positive or negative external effects can be driven out by costless negotiation. Immaterial resources like information, knowledge and ideas inherently carry positive external effects. The complete allocation of property rights of these resources to only one agent is very difficult and sometimes only possible with prohibitively high transaction costs (e.g. costs for patent identification, copyright application, and enforcement). This problem is magnified due to the wide diffusion of the internet in combination with easy-to-use peer-to-peer-file sharing, allowing copying and distribution of digitised files without compensation for the rights holder.⁷²⁵

The introduction of digital rights management systems (DRM), meaning all legal and technical components allowing protection and enforcement of digital rights, offers the possibility of an unambiguous allocation and enforcement of property rights for digital goods with very little transaction costs. For example, functioning DRM technology in combination with appropriately enforced law, e.g. the Digital Millennium Copyright Act (DMCA), helps rights holders of digitised goods to control access rights to content or to charge for use throughout the distribution process. Thus — following *Coase* — well functioning and easy-to-use DRM systems would help to arrive at an efficient outcome with almost no externalities when it comes to production and distribution of digitised goods.

On the other hand, it is often argued that severe protection mechanisms that are beneficial for the individual, i.e. the innovator/rights holder, are an obstacle to the innovative capacity of the total system.⁷²⁶ This is due to the fact that cooperation among agents is limited because free and fruitful information exchange cannot take place, cooperation advantages cannot be realised and inefficient double inventions occur leading to a society with insufficient immaterial resources. Examples like the Open Source Movement or the Scientific Community show that due to open source code and worldwide exchange of ideas, faster correction of errors, wider applicability and faster adoption can be realized compared to closed/proprietary systems. Thus a DRM system that is efficient from the point

in that year it was stated that every novel idea whose realization or development can become useful to society belongs primarily to him who conceived it, and that it would be a violation of the rights of man in their very essence if an industrial invention were not regarded as the property of its creator.” It is however important to realize, that patent law protects the fundamental idea, and copyright law only protects the expression thus not protecting against accidental duplication of the copyrighted work; see e.g.: Landes, Posner (1989).

⁷²⁴ See: *Coase* (1960).

⁷²⁵ See: *Picot, Ripperger, Wolff* (1996).

⁷²⁶ See for an account of the copyright and patent controversy e.g.: *Machlup, Penrose* (1950); *Plant* (1934).

of view of the rights holder may not be socially efficient. This situation can be visualized as a prisoners’ dilemma (fig. 1). Everybody would be better off if weak protection through DRM systems was chosen, but it is only rational for the individual actor to choose strong protection by DRM systems to maximize her profit. Thus, the resulting solution is inefficient for the total system.

		Company 2	
		Weak protection through DRMS	Perfect protection through DRMS
Company 1	Weak protection through DRMS	5 / 5	10 / 1
	Perfect protection through DRMS	1 / 10	3 / 3

Fig. 1. Digital Rights Management Systems’ Prisoner Dilemma

It is this conflict between the calculus of the individual and the total system which leads to a debate about the impact of digital rights management systems on digitised internet based innovation.⁷²⁷

This article investigates positive and negative effects of DRM systems on internet based innovation. It is structured in four sections. The following section two analyses the positive and negative impacts of digital rights management systems on internet-based innovation. Section three recommends general strategies for the design of digital rights management systems and section four concludes the article.

II Favourable and Limiting Impacts of DRM on Internet Based Innovation

Impacts of DRM on innovation can be analysed with respect to the quantity and the type of innovation done.

⁷²⁷ This conflict resembles very much the patent controversy of former centuries. See e.g.: Machlup, Penrose (1950): 35: “*The patent opponents were thoroughly convinced that the patent laws had a harmful influence on the nation at large, and they concluded that their repeal would be beneficial. The patent advocates, on the other side, were ‘thoroughly convinced that the patent laws have a beneficial influence on the nation at large’ and concluded ‘that to repeal them would be suicidal.’*” (quoting from an article of Westminster Review from October 1864).

II.1 Favourable Impacts of DRM on Internet Based Innovation

a) DRM Leads to a Higher Quantitative Level of Innovation

According to the “CSI/FBI 2002 Computer crime and security survey”, the theft of proprietary information costs US business 171 billion US\$ per year.⁷²⁸ This represents an increase of over 800 percent since 1997. Since protecting digital content in the internet is becoming increasingly difficult and up to 70 percent of all expenditures on innovation in industrialized countries are done by profit-seeking companies,⁷²⁹ DRM increases the probability of an inventions’s economic exploitation and therefore can lead to a higher motivation for invention. Also, along with a better funding situation, there is a higher potential to convert ideas into products. If an inventor can’t recover her costs of creation, she probably won’t produce anything.⁷³⁰ This is even more important as innovations involve a high degree of uncertainty with respect to estimating incurring costs and future demand as basis for cash flows.⁷³¹

Considering the higher motivation for invention and the higher probability for realization, DRM can lead to a higher level of innovative activity.

Risk increases with rising costs. Therefore DRM is especially important in case of costly innovations. Considering this fact, it is understandable that Hollywood studios fight so strongly for DRM systems.⁷³² Contrary to the creation of music, which can be done quite cheaply in most cases,⁷³³ the production of a film (=invention) is far more expensive and endangered if amortisation possibilities are reduced. Thus, if the same happened to the film industry as to the music branch, the character of produced films would most likely change completely. Who would produce expensive films with limited merchandising possibilities,⁷³⁴ if they could be downloaded in very good quality with very little costs or without the need to pay for it?

Critics could claim that this kind of argument has already been raised twenty years ago with the invention of the video recorder, whereas cinemas worldwide are obviously still operating. One could argue that peer-to-peer file sharing could also lead to new ways of achieving profits, which have not been discovered so far.

⁷²⁸ See: Powell (2002): 10–11.

⁷²⁹ See e.g.: Bloom, Griffith (2001): 340.

⁷³⁰ See e.g.: Barzel (1968), who suggests that inefficient rapid depletion of a resource could be solved if technological monopoly claims could be granted or auctioned off, giving the owner the exclusive right to develop the technological opportunity.

⁷³¹ See: Landes, Posner (1989).

⁷³² See e.g.: Dykstra (2002): 30: “*The Hollywood industry had spent \$37 million on political contributions and on lobbying Congress during the last election cycle.*”

⁷³³ Even so a music peace starts to become profitable with more than 200.000 copies sold (see e.g.: Gillmor (2002): 74) this is not because of the invention itself, but because of the high exploitation cost.

⁷³⁴ Meaning other than selling the rights of the film. Of course, if there are merchandising possibilities like selling toys or gimmicks, the cash flow from the film itself gets less important.

However, compared to the diffusion of global file sharing, video taping options were much less available and more costly than dvd burning possibilities nowadays.

b) DRM Leads to a Greater Variety of Innovation

Innovation is crucially connected to the advantage an innovator expects from the creation.⁷³⁵ However, the expected gain differs depending on the innovator's preferences. Private software developers or scientific researchers expect reputation and mentioning of their works. Commercial companies on the other hand expect profit generating opportunities. Therefore mandatory DRM systems are beneficial for inventors wanting an exclusive rights position, whereas they are obstructive to inventors interested in wide and fast distribution of their ideas.

Without the existence of DRM systems profit-seeking agents will look for "work-arounds" to protect their own resources. Therefore, without protection mechanisms granting exclusive exploitation rights for a limited period of time there could be a tendency for innovations that are inherently secretive or short-lifecycle. This is supported by Moser⁷³⁶: "The absence of patent laws guides innovative activity towards industries where mechanisms other than patent laws can protect intellectual property. Histograms of exhibition data and predicted values from multinomial regressions show that countries without patent laws have significantly larger shares of their exhibits in industries where patenting rates are low and where contemporary sources describe the use of secrecy."

II.2 Limiting Impacts of DRM on Internet Based Innovation

In recent years, the enforcement of copyright was not very profound with respect to digitised internet based inventions. However, there seems to be no lack of supply of inventive activities.⁷³⁷ On the contrary, the last ten years showed an "explosion" of immaterial resources. This gives rise to the assumption that DRM systems which would enforce property rights to a much higher degree could obstruct innovation. The following arguments are most popular in this context:

a) DRM Systems Jeopardize Fair Use, First Sale, and Time-Limited Monopoly Rights

Copyright and patent laws help the author to exclusively profit from his idea. In most industrialized countries they also promote norms like "fair use", "first sale" and "time-limited protection".

⁷³⁵ Even individuals that are working seemingly altruistic for "free" expect a certain kind of gratification for their work; see e.g.: Raymond (1998); Lakhani, von Hippel (2000); Fiedler (2002) for a summary on the motivations of open source software developers or Andreoni (1988); Andreoni (1990) for motivations that lead to public good contributions. Pure altruism in the sense, that the actor doesn't expect anything for his donation hardly ever happens.

⁷³⁶ See: Moser (2002): 5.

⁷³⁷ See e.g.: Barlow (1994).

“Fair use” refers to the right to reproduce at least some limited portion of a copyrighted work for legitimate purposes, including critical commentary, scientific study, or even parody or satire.⁷³⁸ In other words, fair use enables an agent to quote from previous works in order to comment or report news about them.⁷³⁹

The “first sale” rule is a limitation on the right of rights holders to control copies of their works that have been distributed to the public. This rule stipulates that the first sale of a writer’s copy to a member of the public “exhausts” the rights holder’s ability to control further distribution of that copy. A library is, thus, free to lend or even rent or sell its copies of books to its members. Bookstores, art galleries, and auction houses also depend on it, as does the practice of sharing copies of books or magazines with friends or of giving purchased books to friends.⁷⁴⁰

Also, copyrighted and patented material is only protected for a limited period of time. Or, as the U.S. Supreme Court noted in its decision in “Sony Corp of America v. Universal City Studios”: “the monopoly privileges that Congress may authorize are neither unlimited nor primarily designed to promote a special private benefit. Rather, the limited grant is a means by which an important public purpose may be achieved.”⁷⁴¹

Contrary to this, the combination of DRM technologies and legal norms like the Digital Millennium Copyright Act do not grant these rights to the public. DRM systems enable right holders to protect their material in a way that has never been possible with copyright law alone.⁷⁴² Other than Copyright or patent laws, which promote together with the above stated norms access of the public to copyrighted works, the combination of DRM technology and law can principally stop public access with open end. Many authors state their concern that this would lead to a gradual concentration around certain trusted platforms that cannot be bypassed.⁷⁴³

The most prominent legal DRM regulations in this context are the rules of “anticircumvention” and of “antidevice” laid down in the Digital Millennium Copyright Act (DMCA). The former outlaws circumventing technical protection measures used by rights holders to control access to their works. The latter outlaws devices designed or produced primarily for purposes of circumventing

⁷³⁸ See e.g.: Committee on Intellectual Property Rights and the Emerging Information Infrastructure, (2000): chap. 4, p. 1.

⁷³⁹ The European Union (EU) promotes not the “fair use” right but the very similar “making-available” right (see: Article 3 of the Directive 2001/29/EC in combination with Art. 5).

⁷⁴⁰ See e.g.: Committee on Intellectual Property Rights and the Emerging Information Infrastructure (2000): chap. 3, p. 3.

⁷⁴¹ See e.g.: Committee on Intellectual Property Rights and the Emerging Information Infrastructure (2000): Chap.6. “*Namely providing public access to information and innovative products and services after the period of exclusive control has expired, so as to advance the greater societal good.*”

⁷⁴² See e.g.: Chicola, Farber, Karatsu, Liu, Richter (1998); Lessig (2001); Bechtold (2002).

⁷⁴³ See e.g.: Chicola, Farber, Karatsu, Liu, Richter (1998); Gillmor (2002): 74.

technical protection measures that have no commercially significant uses other than circumvention, or are marketed to circumvent technical protection measures.

Recognizing the criticism, the US-American Congress has acknowledged that circumvention of the Digital Millennium Copyright Act can be done for entirely legitimate purposes such as encryption research, computer security testing, and achieving interoperability for computer systems.⁷⁴⁴ Also, there is a vivid debate concerning DRM and Open Source Software (OSS) development. Supporters of OSS argue, that DRM can kill OSS development, since, for example, it may hinder reverse engineering and interoperability.⁷⁴⁵

b) DRM Systems Are Economically Inefficient

Another main reservation brought forward against DRM systems contends that they are simply inefficient.⁷⁴⁶ Critics state that the granted monopoly rights from patent and copyright laws in combination with DRM systems only raise entry barriers for new innovators with no added value for society.⁷⁴⁷

This is often illustrated with the case of software patents. Due to the possibility to patent software, companies must now consider developing a patent portfolio which can be offered as part of a settlement of third party infringement claims.⁷⁴⁸ Thus, the main importance of software patents is not the acquisition of property rights but the possibility to get access to resources that would be less costly without the option of software patents.⁷⁴⁹

Furthermore, immaterial resources do have inherent positive network externalities that lead towards the creation of natural monopolies (e.g. *Windows*, *Ama-*

⁷⁴⁴ See: Committee on Intellectual Property Rights and the Emerging Information Infrastructure (2000): Chap. 5.

⁷⁴⁵ See e.g.: Gilmore (2001).

⁷⁴⁶ Assuming that they would function in a technically perfect manner which many observers question; see: Biddle, England, Peinado, Willman in this book (page 344).

⁷⁴⁷ See e.g.: Plant (1934): 31: "It is a peculiarity of property rights in patents (and copyrights) that they do not arise out of the scarcity of the objects which become appropriated. They are not a *consequence* of scarcity. They are the deliberate creation of statute law; and whereas in general the institution of private property makes for the preservation of scarce goods, tending (as we might somewhat loosely say to lead us 'to make the most of them,' property rights in patents and copyright make possible the *creation* of a scarcity of the products appropriated which could not otherwise be maintained. Whereas we might expect that public action concerning private property would normally be directed at the prevention of the raising of prices, in these cases the object of the legislation is to confer the power of raising prices by enabling the creation of scarcity. The beneficiary is made the owner of the entire supply of a product for which there may be no easily obtainable substitute. It is the intention of the legislators that he shall be placed in a position to secure an income from the monopoly conferred upon him by restricting the supply in order to raise the price."; Kitch (1986): P.31.

⁷⁴⁸ See e.g.: Savage (1995).

⁷⁴⁹ See: Bessen, Hunt (2003).

zon, *Ebay*)⁷⁵⁰. Once a product or system sets the de-facto standard, digital rights management enhances this effect by making it even more difficult for new firms to attack. As monopolists do not have to defend themselves against competitors, the incentive for investment in research and development is very low.⁷⁵¹ This is especially problematic since the low entry barriers of the internet have the potential to attract a whole new set of participants with other preferences than classic economic agents (e.g. fun instead of profit) who are able to contribute valuable content. Examples are open-source software development, peer-to-peer file-sharing, price search engines and internet auctions. All of these examples have further implications for innovation. Take for example internet auctions. They have promoted enlargement of existing auctioneers like *Sothebys.com*, new auctioneers like *Ebay*, *Amazon* and *Yahoo*, new meta search bots like *bidders edge*, new user strategies concerning buying due to different auction styles, new auction consultants and services like *esnipe*, new law (for example trespass for search agents) and new opportunities for companies, e.g. they can auction their overcapacity on the market.⁷⁵² Had some procedures of internet auctions been protected by DRM this flourishing scene had not developed.

Now, some may argue that without DRM new innovators can enter the market, but without protection of their goods they are not motivated to enter. As shown before, this could be the case, but there are also other results refuting that sort of argument. On the one hand, *Cohen and Levinthal* show that companies invest in research and development even if they know that imitators will also profit from their invention. They explain this with the interest of the firm to enhance its absorptive capacity.⁷⁵³ On the other hand, *Bloom and Griffiths* report that higher education accounts for about one fifth of all R&D done.⁷⁵⁴ This sort of invention is motivated by a love of knowledge, satisfaction gained from puzzle-solving and most of all longing to establishing priority and status.⁷⁵⁵

III Recommendations

Future solutions must find a balance between motivating the innovator and a socially efficient outcome for the public. It may be useful to start from what the law is attempting to achieve — protecting progress of the sciences and arts — and investigate whether the use of a work is frustrating to the author.⁷⁵⁶ On the other hand, a high degree of innovation is only possible with great opportunities

⁷⁵⁰ See: Zerdick, Picot, Schrape, et. al. (2000): 107f. for the Laws of Sarnoff, Reed and Metcalfe.

⁷⁵¹ See e.g.: Shavell, Ypersele (2001); Dixon, Greenhalgh (2002): 5.

⁷⁵² See e.g.: Lessig (2001) for further examples.

⁷⁵³ See: Cohen, Levinthal (1990).

⁷⁵⁴ See: Bloom, Griffith (2001); Dixon, Greenhalgh (2002): 31.

⁷⁵⁵ See: Dixon, Greenhalgh (2002): 31.

⁷⁵⁶ See e.g.: Plant (1934): 36. Committee on Intellectual Property Rights and the Emerging Information Infrastructure (2000): chap. 4, p. 19; Teece (1998); North (1991): 3f: “*Institutions reduce uncertainty by providing a structure to everyday life. They are a guide to human interaction,*

of getting access to new information and ideas. The tradition of providing — for a limited period of time — access to published materials that have been established in the world of physical artefacts must be adequately continued in the digital context.⁷⁵⁷ But the mechanisms for achieving this access and the equivalent of “limited period” will need to evolve in response to the attributes of digital intellectual property and the information infrastructure.⁷⁵⁷

a) Preference Building

Even so “free” peer-to-peer copying is very popular among users of the internet it can be assumed that most people don’t want to break copyright law deliberately. Research shows that a lot of people have a preference for fairness.⁷⁵⁸ Therefore the public should be educated about Copyright in a way that appeals to their fairness preference. This, of course, is a long term undertaking and is quite difficult, especially if business models are perceived as unfair, i.e. too expensive or too limited in use.⁷⁵⁹ Copyright instruction in combination with business models perceived as fair and useful could lead to less piracy and more acceptance of the law. Public compliance with intellectual property law requires a high degree of simplicity, clarity, straightforwardness, and comprehensibility to all aspects of copyright law dealing with individual behaviour. New or revised intellectual property laws should be drafted accordingly.⁷⁶⁰

b) Legal Design

The fool-proof mechanism of laws like the Digital Millennium Copyright Act (DMCA) to complement technical DRM systems is subject to a lot of criticism in the sense that it may obstruct an evolutionary process to achieve a socially efficient solution of the balance to be struck.⁷⁶¹

To offer a balance between individual and collective interests legal solutions must at least protect fair use and enable competition. Therefore the copying of digital information for archival or scientific needs and personalised purposes should be legal.⁷⁶² Also a lot of people claim that circumvention of access controls for fair

so that when we wish to greet friends on the street, drive an automobile, buy oranges, borrow money, form a business, bury our dead, or whatever, we know (or can learn easily) how to perform these tasks.”

⁷⁵⁷ See: Committee on Intellectual Property Rights and the Emerging Information Infrastructure (2000): chap. 6, p. 3.

⁷⁵⁸ See e.g.: Güth (1995): 329ff; Roth (1995): 287ff; Kagel, Kim, Moser (1996): 100ff; Henrich, Smith (1999): 5; Fehr, Gächter (2000): 159ff; Yang, Weimann, Mitropoulos (2002): 6ff.

⁷⁵⁹ See: *Biddle, England, Peinado, Willman* within this book on page 344.

⁷⁶⁰ See e.g.: Committee on Intellectual Property Rights and the Emerging Information Infrastructure (2000): chap. 6, p. 33.

⁷⁶¹ See: Doherty (2002): 68; Bechtold (2002).

⁷⁶² See e.g.: Committee on Intellectual Property Rights and the Emerging Information Infrastructure (2000): chap. 6, p. 11.

use should be legal.⁷⁶³ Or, as the Committee on Intellectual Property Rights states it:

*“This broader review of the regulations is justified because of their unprecedented character; their breadth; and widespread concerns about their potential for negative impacts on public access to information, on the ability of legitimate users to make noninfringing uses of copyrighted works, on research and development in security technology, and on competition and innovation in the high-technology sector.”*⁷⁶⁴

A third way suggests the legal enforcement of discriminatory pricing for data and information to allow educators, scholars and researchers to invoke “fair use” exemptions from the requirements for licensing material that is copyrighted or otherwise legally protected by statute.⁷⁶⁵ However, since the standards for fair use are quite vague, and the enforceability is quite difficult, it seems hard to establish.⁷⁶⁶

Lessig suggests that work an author publishes should be protected for a term of five years once registered, and that registration can be renewed fifteen times. If the registration is not renewed, then the work falls into the public domain.⁷⁶⁷ As the lifecycle of software is shorter, he demands software protection for a term of five years, only once renewable. This protection should be granted only if the author submitted a copy of the source code to be held in escrow while the work was protected.⁷⁶⁸ Once the copyright expired, that escrowed copy would be publicly available from the U.S. Copyright Office server.⁷⁶⁸ Furthermore he suggests that US Congress should limit the reactive character of copyright law. While in the ordinary case the copyright holder should not have to prove harm before enforcing a copyright in a context of significant technological change, a defendant should at least have the opportunity to show that the copyright holder will suffer no harm.⁷⁶⁹ Finally, *Lessig* wants that fees for file sharing are not set by the industry, but by a policy maker keen on striking a balance between interests of the individual and the total system.⁷⁷⁰

c) Business Solutions

Obviously, when the cost of making equivalent copies is higher for the copying person than the price to buy it, the right holder will be able to charge a price higher than her marginal cost, even without legal protection.⁷⁷¹

⁷⁶³ See e.g.: Chicola, Farber, Karatsu, Liu, Richter (1998): 39; Committee on Intellectual Property Rights and the Emerging Information Infrastructure (2000): chap. 6, p. 21.

⁷⁶⁴ See e.g.: Committee on Intellectual Property Rights and the Emerging Information Infrastructure (2000): chap. 6, p. 22.

⁷⁶⁵ See: Chicola, Farber, Karatsu, Liu, Richter (1998): 39; David (2000): 13.

⁷⁶⁶ See: Chicola, Farber, Karatsu, Liu, Richter (1998): 39; David (2000): 40.

⁷⁶⁷ See: Lessig (2001): 251.

⁷⁶⁸ See: Lessig (2001): 253.

⁷⁶⁹ See: Lessig (2001): 254.

⁷⁷⁰ See: Lessig (2001): 255.

But companies do not only have the choice to implement DRM systems to boost the cost of copying. On the contrary, companies can lose in business because they choose a Digital Rights Management technology that is too sophisticated or too expensive just as easily as they can make losses choosing one that is too weak a solution.⁷⁷²

They can also lower the price to buy a copyrighted work. *Biddle, England, Peinado, Willman* suggest that successful business models for digitised goods compete with more customer value consisting in more convenience, higher quality and lower costs rather than additional security.⁷⁷³ A good example of how to survive with digital innovation without DRM solutions are commercial companies that are doing business with Open Source Software. The following table illustrates Open Source Software business models with examples of profit-seeking companies:

Business model	Description	Examples
Support Seller	Revenue comes from media distribution, branding, training, consulting, custom development, and post-sales support instead of traditional software licensing fees	GNU/Linux Distributors: Red Hat Inc., SuSE, Caldera Systems Inc., Mandrake, Pacific HiTech, Alcove: GNU/Linux, CVS, Debian, Exim, FreeBSD, IMP, MySQL, PostgreSQL, OpenLDAP, Perl, PHP, Samba, Squid, Sympa, Zope CollabNet: SourceCast Enhydra: Enhydra application server SourceGear: AbiWord e.g. AbiSource, Linuxcare: Gnu/Linux MySQL: MySQL, PostgreSQL: PostgreSQL
Loss Leader	A no-charge open-source product is used as a loss leader for traditional commercial software.	Sendmail Inc.: Sendmail, SAP: SAPDB
Hardware Add-On ('Widget frosting')	For companies that are in business primarily to sell hardware but which use the open-source model for enabling software such as driver and interface code.	<ul style="list-style-type: none"> • Cyclades, • IBM, • Hewlett Packard, • Penguin Computing, • Sun, • VA Linux Systems

⁷⁷¹ See: Landes, Posner (1989).

⁷⁷² See: Committee on Intellectual Property Rights and the Emerging Information Infrastructure (2000): chap. 5, p. 24; *Biddle, England, Peinado, Willman* within this book on page 344.

⁷⁷³ See: *Biddle, England, Peinado, Willman* within this book on page 344.

Access- orizing	For companies which distribute books, computer hardware and other physical items associated with and supportive of open-source software.	O'Reilly & Associates Inc., SuSE
Service Enabler	Where open-source software is created and distributed primarily to support access to revenue-generating on-line services.	Netscape Netcenter Services: Netscape Communicator,
Brand Li- censing	A company charges other companies for the right to use its brand names and trademarks in creating derivative products.	Netscape Communication Corporation Netscape Communicator (only Netscape is using this name, all others have to use the name Mozilla)
Sell It, Free It	A company's software products start out their product life cycle as traditional commercial products and then are continually converted to open-source products when appropriate.	Aladdin: Ghostscript, Apple: Darwin, Cisco: CEPS, Dresdner Kleinwort Wasserstein: Openadaptor, Ebuilt: Flood, IdSoftware: Doom HewlettPackard: CoolTown, IBM: Eclipse, Jikes, Netscape: Mozilla, Sun: Open Office, Sun Grid Engine, JXTA, Net Beans
Software Franchising	A combination of several of the preceding models (in particular "Brand Licensing" and "Support Sellers") in which a company authorizes others to use its brand names and trademarks in creating associated organizations doing custom software development in particular geographic areas or vertical markets, and supplies franchises with training and related services in exchange for franchise fees of some sort.	Transgaming.com: WineX, Cosource.com.
Hybrid Models	Hybrid models relax the constraints surrounding open source in one way or another. For example, a company might use both traditional licensing and open-source-like licensing "side by side" for the same product, differentiating between different users	StaticFreeSoft: Electric VLSI Design System,

Fig. 2. Open Source Software Business Models⁷⁴

There are, of course, limits to the applicability of these business models. Most of them are not profitable yet and others are not yet discovered. The business model must be carefully matched to the product. While the appropriate business model can render the need for technical protection obsolete for some products, for some other products substantial protection might be necessary.⁷⁷⁵

IV Conclusion

As the internet shifts balance towards society, DRM systems shift balance towards the rights holder of the invention. Obviously, inventors do have to benefit from their invention in some way. But this benefit varies with the inventors' preferences. For example, scientists maximize their utility by being quoted, private Open Source Software developers by the use of their product, the help of others and reputational gains, or companies by earning additional revenue. Therefore, it is more efficient for the total system to find a balance between inventor gratification and free use by society than to concentrate solely on strengthening DRM systems.

Apparently, profit-seeking inventors must have a chance to profit from their invested resources in research and development. But this does not mean that they have to profit from it for an unlimited time or unlimited amount. DRM will be most beneficial in innovation areas, which demand high financial investment, since they attract mainly profit-seeking inventors. However, areas which attract people with other preferences than pure profit-seeking and which require only low financial investments will most probably flourish more with a weak digital rights management system. Therefore, legal measures such as software patents and anticircumvention regulations should be implemented with great care. At the same time, it should be up to the inventor how she wants to protect her works technically. Even with technical protection tools in action, the provision of fair use can be implemented with the rule that digitised works have to be submitted to a publicly-accessible library. Finally creators/rights holders should not only rely on DRM systems, but should also consider business models allowing the generation of profits.

⁷⁷⁴ Adapted from Hecker (1999) and Henkel (2002).

⁷⁷⁵ See: Committee on Intellectual Property Rights and the Emerging Information Infrastructure (2000): chap. 6, p. 23.

3.5 Evaluating Consumer Acceptance for Protected Digital Content

*Marc Fetscherin*⁷⁷⁶

Abstract: This paper argues that content providers must overcome three hurdles to establish a viable business model for monetizing copyrighted digital content on the Internet. First, content providers must change perspectives to view the pirating of their content as a competitive threat and not just as theft. This implies they must learn to compete against pirated versions of their own products. Second, content providers must come to view the Internet as a new distribution channel that is fundamentally different from any they have used to date. Accordingly, they must accept that this new distribution channel differs from their existing channels with its specific consumer behavior, needs and willingness to pay. Finally, content providers need to gain insight into the impact of channel controls, such as protection technologies, on consumer adoption. Thus, content providers need to find the threshold for how much protection technology consumers are willing to accept for paid digital content.

I Introduction

We are approaching the third era of the Internet and digital content. The first era was marked by extensive distribution of free information and services in a battle for consumer “eyeballs”, with the hope of sustained advertising revenues and eventual profitability. The search for viable business models for digital content, with the bursting of the dot.com bubble, marked the second era. The third era will represent the emergence of viable business models, a significant decline in the amount of free high quality content, and new revenue streams that include charging consumers for digital content⁷⁷⁷.

Over the last ten years, technology advances — including hardware advances like CD-R (w), scanners, or high speed modems and software advances in compression formats like MP3 and MPEG — have enabled individuals to quickly and cheaply digitize, store, share, and modify digital content on a mass scale. The emergence of IT-networks such as the Internet provides a fast, cheap and global distribution channel⁷⁷⁸. The combination of these reproduction and distribution technologies leaves individuals with numerous methods and channels through which to access and provide digital content. Therefore, individuals can act as both consumer and provider (whether legal or illegal) of digital content⁷⁷⁹. These modern technologies have also enabled individuals to produce perfect copies of digital and non-digital content without the involvement of content providers. Finally, in the analogue world individuals had to spent money and time to copy content on a physical media (e.g., buy a cassette). In contrast, in the digital world copying is a more background process that leaves acquiring and sharing

⁷⁷⁶ Institute of Information Systems, University of Bern.

⁷⁷⁷ See: Hurd (2001).

⁷⁷⁸ See: Bechtold (2002).

⁷⁷⁹ See: Haug, Weber (2002).

digital content, whether legally or illegally, a relatively costless activity for individuals. However, in the digital world content providers are those who have to spend money in order to prevent such copies.

The result has been the desegregation of the value chain, an increasing amount of digital content available — legally or illegally. This poses an enormous threat for content providers, as those are authorized to only provide copyrighted digital content. So far, most content providers of media and entertainment content such as music, movies, or games have not been successful or profitable in charging consumers for their content despite the huge latent demand⁷⁸⁰. Nor have they been successful in creating the technology frameworks, such as the use of Digital Rights Management Systems, required to remunerate content owners and protect against piracy primarily because individuals have widely resisted.

In the current literature the issue of consumer acceptance of protection technologies or the consumer acceptance of protected digital content is treated very little. Some researchers or studies touch this topic partially or make some short comments about, but none of them is devoted to this issue an entire report or analysis. This paper wants to close that gap by making a first step towards structuring and understanding this issue. The author wants to explore the topic in detail and argues that content providers must overcome three hurdles to address the technology realities discussed above and to capture this huge, potential demand of copyrighted digital content. The three hurdles are:

- 1) Learning to compete against pirated versions of their own product.
- 2) Seeing online distribution as a new channel, distinct from their traditional channels, with a different consumer behavior, need and willingness to pay.
- 3) Finding the equilibrium between digital protection technologies and the consumers' desire for hassle-free purchase, ownership, and consumption.

II The First Hurdle: Competing against Pirated Versions of Their Own Products

This section defines Internet piracy, outlines the motivations for stealing digital content, and argues that content providers must accept electronic theft of their intellectual property as the unchangeable reality and learn to compete with pirated versions of their own products. This section goes on to analyze consumer preferences for digital content and concludes by suggesting a model for how content providers can compete against pirated versions of their content, and what are the options in order to shift the illegal demand to legitimate purchases.

II.1 Internet Piracy

A detailed discussion about Internet piracy is out of the scope of this paper. However, some background is necessary. Although the content industry argues that piracy costs them several billion USD a year⁷⁸¹, there is no empirical evidence

⁷⁸⁰ See: SIIA & KPMG (2001).

to support their claim. There is even contrary research from industry analysts, such as Forrester, Media Matrix, and authorssmall like Liebowitz⁷⁸², Hui⁷⁸³, and Cave⁷⁸⁴ which show the suggest cost of piracy is statistically unsupported and is unlikely to be as high as the content industry claims. What is not in debate is that millions of people are sharing billions of copyrighted digital content through the Internet on a mass scale⁷⁸⁵. Napster, KaZaA or other peer-to-peer networks are only a few examples that illustrate this huge mass illegal copying and sharing. The question of why individuals steal copyrighted material is very difficult to answer and only limited empirical evidence exists within the literature⁷⁸⁶. As mentioned in the introduction, technology advances have enabled low reproduction costs⁷⁸⁷, while the Internet provides low distribution costs. This powerful combination allows individuals to access, copy, and to share virtually any type of digital content without cost or time delay. This underscores one argument put fourth in the literature that individuals steal content because it is easy, quick and cheap for them.

Another argument might be that people have always copied and shared things in the past and will do so in the future, especially when CD-, DVD (re)-writables and network connectivity become mainstream for example. Finally, according to a recent publication, presented at the DRM conference in Washington in November 2002, from well know researches of Microsoft received huge public exposure. The reasons being that they are the first to admit that content providers have to live with Internet piracy or as they named it, the darknet. They define the darknet as a collection of networks and technologies used to copy and share digital content. Examples of darknets are peer-to-peer file sharing, CD and DVD copying, and key or password sharing on e-mail and newsgroup. The authors of this text⁷⁸⁸ believe that the darknet will continue to grow and provides low cost, high quality services to a large group of consumers. In short, they argued that in many markets, the darknet will be a direct competitor to legal purchases and content providers must learn to accept this as reality.

II.2 Consumer Preferences: Two Competing Acquisition Routes

Individuals have a variety of possibilities to acquire digital content legally or illegally. Taking an example from the media and entertainment industry (e.g., music files, movies, or games) an individual can purchase it legally by downloading or streaming it from a web site such as Pressplay or Movielink. He also has the possibility of getting it illegally through web sites or through peer-to-peer

⁷⁸¹ See: IFPI (2002). SIIA (2001).

⁷⁸² See: Liebowitz (2002).

⁷⁸³ See: Hui (2002).

⁷⁸⁴ See: Cave (2002).

⁷⁸⁵ See: Fetscherin (2002).

⁷⁸⁶ See: Takeyama (2002); Hui (2002); Holm (2000).

⁷⁸⁷ See: Yoon (2001).

⁷⁸⁸ See: *Biddle, England, Peinado, Willman* within this book on page 344.

networks such as KaZaA or Morpheus. Thus, individuals have two possibilities to get digital content, buy the digital content legally or acquire it illegally. What follows is a model for exploring the tradeoffs an individual faces between legal and illegal content acquisition. This model excludes the possibility that an individual does not want digital content and its logic will be used to support arguments throughout the remain of this paper. *Note: there is a major obstacle to these studies because the behavior under study (i.e., piracy) is an illegal activity, which limits the amount of official market data that is available*⁷⁸⁹.

Suppose digital content is developed and there are individuals who desire to acquire it. Assume that each individual wants either zero or one unit of the content and that he makes an independent decision between legal and illegal acquisition of the content. Let's denote the set of individuals by I and the valuation, or the perceived value of the content, for a given individual (i) as v_i where a normal distribution is assumed. Let's also denote the perceived value that the individual places on acquiring the original, as opposed to a copy, by vo_i .

Acquisition costs include three parts. First, the data communications costs to be paid to a telecommunication company and/or an Internet Service Provider (e.g., access costs, cost for searching, downloading), second the media storage costs (e.g., hard disk), and third the price to be paid for the original. It is assume the communication costs and storage costs are equal for both legal and illegal acquisition and therefore are omitted from the model. The only cost an individual has for a legal purchase is the price for the original. Thus, we have:

- $I \hat{=}$ The Number of Individuals
- $vo_i \hat{=}$ Perceived value the individual places on the original
- $p \hat{=}$ The Price for the original

Legal Acquisition

The first possibility an individual has is the acquisition of the digital content through legal purchase. In this case, the individual pays the price p . Assume $vo_i, p \geq 0$. Thus, the net benefit the individual receives can be presented as follows:

$$vo_i - p \hat{=} \text{net benefit} \quad (1)$$

Illegal Acquisition

The alternative to the model above is for the individual to acquire the digital content as an illegal unauthorized copy. If the individual copies the item illegally, he enjoys a benefit of $vo_i (1 - \delta)$ instead of vo_i where $0 \leq \delta \leq 1$ captures the quality differential between the original and the copy. When δ equals zero, the copy is perceived as a perfect substitute to the original. The more δ tends to one, the higher the perceived quality difference between the original and the copy. The reasons a copy may not be as good as the original is

⁷⁸⁹ See: Holm (2000).

due to quality degradation, the lack of manuals, or the lack of technical support⁷⁹⁰. Let vc_i represent $vo_i(1 - \delta)$ for the perceived value the individual places on the copy.

Assume that each individual incurs copying costs when making a copy of the content. These costs are comprised of different components such as time to copy, effort to copy, and the risk of being caught. Time and effort depend on the strength of copyright protection technologies where the risk of being caught depends on the degree of law enforcement. It is assumed that copy protection technologies do not restrict individuals in the usage of the legally acquired digital content and the copy does not include any protection technology, if not it would not exist such copy. Thus, copy protection technology do not restrict individuals in the usage of the illegal copy. Therefore it is not taken into account as a cost. Law enforcement can be presented by the probability μ that the individual will be caught and f for the legal penalty assessed when their theft is detected. Let x represent the expected fine $x = \mu f$. As Harbaugh & Khemka⁷⁹¹ mentioned, enforcement that disrupts distribution channels or limits access to copyrighted content raises the cost of the copy or increases the likelihood that unauthorized copying will be detected and punished.

$\delta \hat{=}$ Captures the quality differential between the original and the copy

$vc_i \hat{=}$ Perceived value the individual places on the copy, $vo_i(1 - \delta)$

$\mu \hat{=}$ Detection rate of piracy (probability that the individual will be caught)

$f \hat{=}$ Legal penalty

$x \hat{=}$ Expected fine ($x = \mu f$)

Thus, the net benefit an individual (i) places on the illegal acquisition is presented as follows:

$$vc_i - x \hat{=} \text{net benefit} \quad (2)$$

By this logic, for an individual to purchase the digital content, it is necessary that equation (1) \geq (2), and $vo_i \geq 0$, which implies:

$$vo_i - p \geq vc_i - x \quad (3)$$

$$vo_i - vc_i \geq p - x \quad (4)$$

II.3 Competing against Pirated Versions of Their Own Products

Independent of the type of digital content (e.g., music, movies, games), the distributed channel used (e.g., Internet, mobile), or the respective consumer group, the model above shows two major factors that content providers can directly influence to shift a portion of the illegal demand to legitimate purchases, thereby successfully competing against their own pirated products. The first is the perceived value by the individuals (v_i) and the second is the price (p) for legitimate

⁷⁹⁰ See: Yoon (2001).

⁷⁹¹ See: Harbaugh, Khemka (2001).

purchase. Content providers can also impact the individual’s perception of the risk of getting caught. If an individual perceives a strong law enforcement with a high chance of prosecution (i.e., μ and $f > 0$, thus $x > 0$) for dealing with illegal copies, he may prefer to legally buy the digital content.

To this end, there are four situations outlined in Figure 1 in which an individual may be situated. He may be in an environment with a perceived weak law enforcement (e.g., Europe, Asia, Africa), or an environment with a perceived strong law enforcement (e.g., U.S.). In addition, the individual may perceive the copy either as a substitute or as an imperfect substitute compared to the original⁷⁹².

		Law Enforcement (costs)	
		Weak ($x = 0$)	Strong ($x > 0$)
Perceived value	Imperfect substitute $vo_i - vc_i > 0$	②	④
	Substitute $vo_i - vc_i = 0$	①	③

Fig. 1. Possible Situations for an Individual

Weak Law Enforcement

In an environment where the individual perceives weak or no law enforcement, the probability of detection is zero, thus $x = 0$. Taking equation (4), p can then be interpreted as how much the individual values the original over the copy. The distribution of this additional willingness to pay for the original will be important for the content provider’s ability to generate profits in the legal markets, where parallel markets for copies are present⁷⁹³. This can be presented as follows:

$$vo_i - vc_i \geq p \tag{5}$$

Let’s now evaluate the two situations shown in Figure 1: the copy perceived as a substitute to the original and copy perceived as an imperfect substitute to the original.

Situation ①: If $vo_i - vc_i = 0$, thus $p = 0$ (copy is perceived as a substitute). In this case, the individual perceives the copy as a substitute to the original. In this situation, decreasing the price of the original will not help content providers to shift a significant part of the illegal demand to legitimate purchases. This leaves content providers with only one option, increasing the perceived value for their original (vo_i) thereby minimize the incentive for individuals to acquire illegal copies. Providing additional value to the original will only benefit the content providers by increasing the gap between the perceived value of the original

⁷⁹² See: Besen, Kirby (1989).

⁷⁹³ See: Holm (2000).

and the now imperfect copy⁷⁹⁴. To compete against their own pirated products, content providers must work to shift from situation ① to situation ②.

Situation ②: If $vo_i - vci > 0$, thus $p > 0$ (copy is perceived as an imperfect substitute). In this case, the individual will value the original more than the copy, thus be willing to pay for the digital content. Where this is the case, content providers have two options. The first is to increase the perceived value and simultaneously increase the price in order to provide the same net benefit to consumers. The second would be to reduce price as a method of increased competition with pirates and in hope of shifting a part from the illegal demand to legitimate purchases.

Strong Law Enforcement

An environment where individuals perceive strong law enforcement. In this case the probability of getting caught μ is greater than 0, with a legal penalty f greater than 0, thus $x > 0$. This case is more complex than those above, for two reasons. The first is that it is very difficult to evaluate μ and f . The second is that this model fails to account for the individuals risk aversion. However, it can be argued that the individual's risk aversion to getting caught is included in the perceived value of the copy (vc_i) (i.e., *ceteribus paribus*, vc_i declines with the increase of the individual risk averseness). Under condition $vo_i > 0$, this implies:

$$vo_i - vci \geq p - x \quad (6)$$

Again, two different situations can be analyzed and are shown in Figure 1: the copy perceived as a substitute to the original and copy perceived as an imperfect substitute to the original.

Situation ③: If $vo_i - vci = 0$, thus $p = x$ (copy is perceived as a substitute). In this case, the individual perceives the value for the copy as a substitute to the original. In addition, the price that the consumer pays for the original equals the costs to acquire the copy (i.e., $x \hat{=}$ expected fine). Content providers have three options for competing against their own pirated products. First, they can increase the perceived value of the original (vo_i), in order to go from situation ③ to situation ④. Second, they can reduce the price, making acquiring the original cheaper than acquiring the copy. Finally, as they are in an environment with a perceived strong law enforcement, they can try to strengthen law enforcement (i.e., increase x which reduces vc_i).

Situation ④: If $vo_i - vci > 0$ (copy is perceived as an imperfect substitute). In this case, individuals value the original more than the copy and content providers again have three options for competing against their own pirated product. First, they can increase the perceived value and simultaneously increase the price in order to provide the same net benefit to consumers. Second, they can use price cuts to cope with pirates and shift a portion from illegal acquisition to legitimate purchases. Finally, as they are in an environment with a strong law enforcement, they can try to strengthen it (i.e., increase x which reduces vc_i).

⁷⁹⁴ See: Gordijn et al. (2000).

A detailed discussion about pricing of digital content (p), and business models (v_i) is out of the scope of this paper and various research has previously explored the topic⁷⁹⁵. This said, some additional comments and conclusions can be drawn from the above model and analysis.

Pricing (p) and the value proposition (v_i) seem to be the most important factors that content providers can directly influence and use to compete against pirated versions of their own products. Ironically, tweaking the pricing factor (p) is not new to the content industry. For example, Hollywood studios learned that by lowering the price of popular VHS movies from ~\$100 to ~\$10 they could make more money. Accordingly, in the last 15 years, video purchase prices have dropped by more than 90 percent, creating both a strong argument and a good example for digital content providers to follow. Indeed, today, the sale of videotape movies generates more revenues than theatrical showings⁷⁹⁶. Another illustration in support of perceived value (v_i) comes from a quick review of ConsumerReports.org. Not only do they provide the same content on the Internet as they do in their subscription magazine, but they create and implement web-only content, such as interactive tools (e.g., search, calculator), to increase the perceived value for individuals⁷⁹⁷.

The perception of strong law enforcement (x) by individuals may reduce Internet piracy. To create this perception, content providers are starting to sue individual's not just organizations. In 2002, copyright holders in the U.S. have routinely been notifying ISP's that their subscribers have been illegally sharing copyrighted files online. In July 2002, the Recording Industry Association of America (RIAA) asked Verizon, a major US internet service provider, for the direct contact information of subscribers⁷⁹⁸. In a federal court decision, Judge John Bales ruled against Verizon and told them to provide the contact information to the RIAA. Verizon has since announced its intention to appeal the decision. Needless to say, these local-level court struggles only underscore that implementing strong law enforcement will be difficult on a global scale. However, by making very public "show cases" (e.g., sue a university, company, and some known individuals), content providers can increase the perception that strong law enforcement exist. If they achieve this goal, individuals may begin to realize that copying and sharing of copyrighted digital content is the same as stealing the CD from a music store. This would be a huge step towards consumer acceptance of paid content.

⁷⁹⁵ See: Äijö, Saarinen (2001); Buhse (2001); Chen (1998); Hui (2002); Kinsely (2001); Mahadevan (2000); McGarvey (2001); Picard (2000); Varian (1995); Shapiro, Varian (1999).

⁷⁹⁶ See: Liebowitz (2002).

⁷⁹⁷ See: Marketing Sherpa Inc. (2002).

⁷⁹⁸ See: Borland (2002).

III The Second Hurdle: Understanding the Consumer Behavior, Needs, and Willingness to Pay

This section reviews consumer behavior in respect to their needs and their willingness to pay for digital content. It begins by reviewing consumer needs for digital content and then argues that an individual's willingness to pay for digital content depends on five factors (5 C's framework). Throughout this section, scientific literature, survey research and case examples are used to illustrate key arguments for where and why individuals are paying for digital content and to underscore the five key factors influencing the willingness to pay for digital content.

III.1 Consumer Needs

A recent study conducted by Ears & Eyes⁷⁹⁹, which evaluated individual willingness to pay for digital content, suggested seven needs or criteria for individuals to find digital content worth purchasing. The study includes responses from more than 1,000 individuals. The results are outlined in Figure 2.

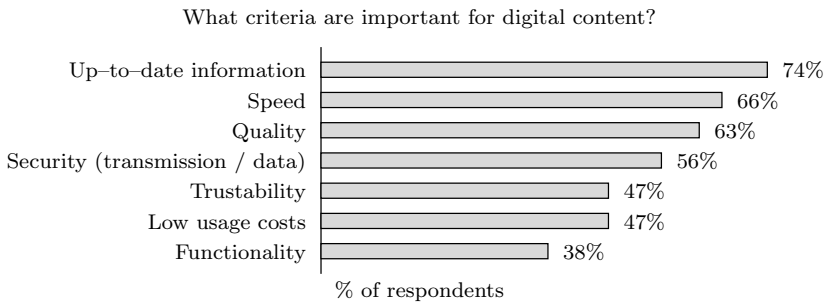


Fig. 2. Individual Purchasing Factors / Criteria for Digital Content

From the survey above, among the top seven needs or buying factors are those related to the way the content is presented (e.g., up-to-date information, functionality) and those related to the way the content is transmitted (e.g., speed, security, quality). This suggests that the best, up-to-date and unique content is of little monetary value if there are technical problems with its transmission or consumption⁸⁰⁰.

It is important to note that individual purchasing factors and criteria vary by the type of content, the distributed channel used, the respective consumer group, and the cultural environment where the consumer group is situated.

⁷⁹⁹ See: Ears & Eyes (2001).

⁸⁰⁰ See: Ears & Eyes (2001).

III.2 Consumer Willingness to Pay

Why are teenagers in Europe willing to pay for short text messages (SMS) over mobile networks but not for e-mail on the Internet? Why do young Americans seem more willing to pay to access on-line text-based archives than music ones? Why do software piracy rates differ from one European country to the next? These are just a few questions content providers are struggling to grasp.

This paper argues that there are five common factors that influence an individual's willingness to pay for digital content. In each of the above-mentioned questions those can be found. Let's take the first question as an example: "Why are teenagers in Europe willing to pay for short text messages (SMS) over mobile networks but not for e-mail on the Internet?" The five factors are as follows. The first factor is the type of content (e.g., text based messages), the second is the consumer group (e.g., teenagers), the third is the channel used to distribute the digital content (e.g., mobile vs. Internet). The fourth factor is the content provider's strategy for pricing and creating perceived value, and the fifth factor is the country / cultural environment (e.g., Europeans). The last two factors were already discussed in detail in the first section of this paper. It should be noted that by changing only one factor, in our case the distribution channel, this has a huge impact on the individual's willingness to pay.

Figure 3 illustrates the 5 C's framework outlining the different factors influencing the willingness to pay.

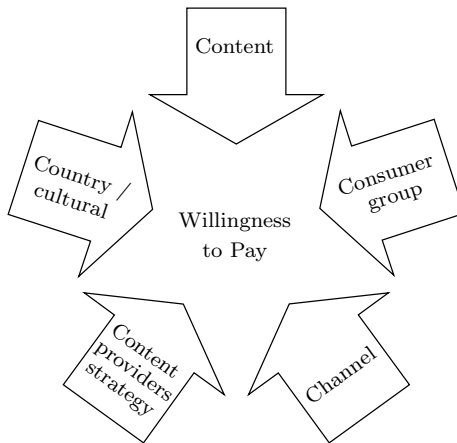


Fig. 3. Five C's Framework

What follows is a more detailed overview of each of the five factors and evidence to support this paper's argument that these five factors are the most important ones influencing an individual's willingness to pay for digital content.

III.3 First Factor — Type of Content

Individuals are spending more time online and are consuming more digital content⁸⁰¹. However, this does not imply that just because individuals are consuming digital content that they are willing to pay for its use. Among others, the research from Ears & Eyes suggests that there is no direct connection between the current usage of digital content (e.g., e-mail, music downloads) and the willingness to pay for it. In addition, this study illustrates that different types of digital content command different price sensitivities and levels of willingness to pay. Figure 4 illustrates how an individual's willingness to pay may vary by type of content. For example, 8 percent of respondents are currently paying for database / archives in contrast to daily news where only 1 percent is currently paying for. Other research from Forrester⁸⁰², Online Publishers Association⁸⁰³, Consumer Electronics Association⁸⁰⁴, and Seybold Research⁸⁰⁵ has come to the same conclusion.

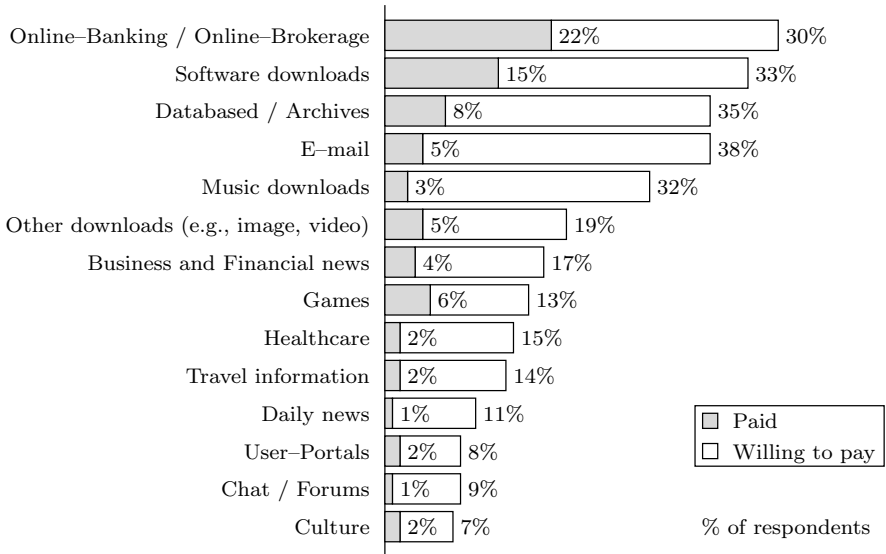


Fig. 4. Willingness to Pay according to Type of Content

The results presented in Figure 4 map almost exactly to the purchasing criteria outlined in Figure 2. Take the example of online-banking / online brokerage. For 22 percent of respondents in Figure 4, online banking / brokerage fulfills their needs for up-to-date information, speed, trustability and low usage costs (cp. Figure 2). In summary, the study by Ears & Eyes among other suggests the type of content offered by content providers plays an important role in determining an individual's willingness to pay.

⁸⁰¹ See: Jupiter Research (2001).

⁸⁰² See: Charron (2002).

⁸⁰³ See: Online Publishers Association (2002).

⁸⁰⁴ See: Wargo (2001).

⁸⁰⁵ See: Seybold Research (2001).

III.4 Second Factor — Consumer Group

Individual willingness to pay for digital content can be differentiated by gender, age group, income, access speed and so on. A detailed description about consumer groups and their willingness to pay is out of the scope of this paper and, as a well-researched area, detailed examples of online consumer segmentation can be found within the literature⁸⁰⁶. This said, to support the argument of this paper, we want to provide examples of how the willingness to pay for digital content differs by consumer group. They may differ:

- By gender: 57 percent of male vs. 34 percent of female have already paid for digital content.
- By age group: 40 percent of individuals between 16 – 19 years old vs. 53 percent of individuals between 20 – 29 years old have paid for digital content.
- By net income: 42 percent of individuals with a net income smaller than €1.500 per month vs. 57 percent of individuals with a net income higher than €2.500 per month have paid for digital content.

In general, the literature shows that the majority of males, older than twenty and with a high net income are more likely to pay for digital content than young females with a low income. Therefore, in order to sell a certain type of digital content distributed over a specific channel (e.g., online banking/brokerage) in a certain cultural environment, content providers have to carefully segment their consumers and target according to their willingness to pay. In our example of online banking/ brokerage, 27 percent of males versus 7 percent of females have already paid for online banking/brokerage⁸⁰⁷. The successful marketing of digital content requires targeting consumer segments based on their willingness to pay.

III.5 Third Factor — Channel Used to Distribute the Digital Content

To the surprise of telecommunication companies and content providers, individuals seem more willing to pay for digital content distributed over mobile networks than through the Internet. There are many possible explanations for this. First, a mobile network is a closed network, thus it is more difficult for individuals to illegally provide and share digital content. Second, billing systems are already in place and are easy to use, which reduces the barrier for individuals to pay for content. Finally, consumers are accustomed to pay for mobile communication, either data transmission or voice transmission. Thus, there is less of a cultural resistance to pay for digital content on a mobile network.

Let's take the example of short text messages (SMS) over mobile networks. Although estimates vary between associations (e.g., GSM Association, Mobile Data Association) or Research houses (e.g., Forrester, Jupiter) the current SMS volume is in the range of several billion messages per month, worldwide. In the UK for the month of July 2002, over 50 millions subscribers sent an average of 40 million SMS per day⁸⁰⁸. Although this is less than one SMS per subscriber

⁸⁰⁶ See: Jupiter Research (2001/2002); PewInternet (2002); IDC (2000a).

⁸⁰⁷ See: Ears & Eyes (2001).

⁸⁰⁸ See: Mobile Data Association (2002).

per day, this usages quickly adds-up and results in more than 1 billion SMS per month with a total of more than 10 billion SMS a year on average for the UK alone. One reason why SMS messages are a success might be that sending a SMS is cheaper than a one minute voice call — and, unlike voice calls, receiving SMS messages is free. This reality forces the consumer to decide if the SMS is a suitable alternative (e.g., substitute) to a one minute call. Although e-mail might be a substitute of a phone call, according to the study from Ears & Eyes only 5 percent of individuals are paying for this (cp. Figure 4). Thus, content providers have to understand that the same or similar digital content might be successfully sold over one distribution channel but not over another. While this example was specific to text based messages, it is equally applicable to music or other forms of digital content.

III.6 Fourth Factor — Content Providers Strategy

As discussed above, a content provider's go-to-market strategy will play a significant role in an individual's willingness to pay for digital content — particularly their pricing model and efforts to create perceived value.

Consider the following example of how pricing impacts consumption. The online magazine Slate switched from free to fee in 1998, when it began charging USD 19.98 per month for access. Shortly thereafter, visitors to their site almost entirely disappeared, and in 1999, Slate went back to the “free” format, saying that it expected more revenues from advertising and marketing of its registered user lists. As a result of this change, traffic increased by 175% in a matter of days⁸⁰⁹.

An example for perceived value can be obtained from a study conducted by Cheng, Sims & Teegen⁸¹⁰. They showed that one important reason for purchasing software, as opposed to stealing it, was the availability of manuals, since copying a software manual increases the cost of pirating or reduces the perceived value of the copy. Therefore providing complementary physical products such as manuals might increase the perceived value of the original. Other factors that contribute to perceived value include brand recognition and content provider's reputation, exclusivity of the content, breadth of content offering, and existing familiarity with the content provided.

III.7 Fifth Factor — Country / Cultural Environment

The model presented in the first section of this paper (cp. Figure 1) has shown that an individual might be in an environment with a perceived weak or perceived strong law enforcement. This perception is not created at a consumer group level (i.e. second factor influencing the willingness to pay) but more on a cultural level where all individuals from the same region or country, thus an aggregation of various consumer groups, would have a similar behavior. Statistics on how

⁸⁰⁹ See: Laudon, Traver (2002).

⁸¹⁰ See: Cheng, Sims, Teegen (1997).

piracy rates differ between countries provide good examples of how the cultural environment influences the willingness to pay for digital content. Moreover, there are many examples within the literature outlining the major determinants of the cultural difference. Example are the capita GDP per country⁸¹¹, people's attitudes toward piracy behavior⁸¹² or peoples attitude towards paying for digital content⁸¹³.

If content providers want to charge individuals for their digital content, they must understand the five factors presented in this section, how they influence directly the willingness to pay as well as how they influence each other. Content providers should be aware that by adjusting or changing only one factor this will already have a significant impact on the markets willingness to pay for digital content.

IV The Third Hurdle: Evaluating Consumer Acceptance for Protected Digital Content

Thus far, this paper has shown how content providers can compete against pirated versions of their own products and to understand the consumer behaviors, needs and willingness to pay. The final hurdle content providers must overcome is finding the equilibrium between digital protection technologies and the consumers' desire for hassle-free purchase, ownership, and consumption.

Protection technologies are a wide variety of software and hardware-based mechanisms that limit access to and usage of digital content⁸¹⁴. There are three broad areas of protection technologies. The first is the protection of the distribution of digital content on physical package media such as CD's or DVD's. The second is the protection of the distribution of digital content in digital format on closed network systems such as cable, satellite or mobile networks. The third is the protection of the distribution of digital content in digital format over the open network Internet⁸¹⁵. This paper focuses on the last one, the consumer acceptance for protection technologies used for digital content distributed over the Internet.

IV.1 Balancing the Competing Interests of Content Providers and Consumers

The difficult tasks of protection technologies, such as Digital Rights Management Systems, is to strike the correct balance between two somewhat contradictory objectives. The first is to give the right incentive to content providers so that digital content can be created in the first place, and second is to promote wide access to and usage of copyrighted works. The difficulty is that increased pro-

⁸¹¹ See: Andres (2002).

⁸¹² See: Cheng, Sims, Teegeen (1997).

⁸¹³ See: Laudon, Traver (2002).

⁸¹⁴ See: Committee on Intellectual Property Rights and the Emerging Information Infrastructure (2000).

⁸¹⁵ See: Wargo (2001).

tection will increase the social welfare by ensuring and monetary reward and inducing more creative works to be produced, but it will decrease the social welfare by limiting or restricting how lawful consumers can use and consume the content⁸¹⁶. Thus, the most challenging issue for content providers is finding the balance between these two contradictory objectives.

IV.2 Consumer Acceptance for Protection Technologies

The software industry, which loses according to the Software Information Industry Association⁸¹⁷ over \$12 billion a year from piracy, provides a good example into this trade-off. Thus far, and despite many attempts, the software industry cannot get the market to accept copy protection technologies. No mass-market software publisher would risk shipping copy-protected software, consumers seem to hate it and all attempts have failed to stop hackers from pirating⁸¹⁸. The question is why? The standard answer is that company would sell less and would be more vulnerable to legal or illegal competition. Thus, if protection technologies for packaged media have faced significant resistance, it seems less likely that such technology would gain wide consumer acceptance for the protection of content in digital format distributed over the open, unsecure Internet. However, although it is too early to draw any conclusion about the protection technology concept used with the latest Microsoft product Windows XP, it has the potential of a higher consumer acceptance.

One of the main problems with protection technologies is that it is primarily concerned with the illegal usage of material and cares little and even hinders the lawful consumers. Accordingly, content providers must ensure that legitimate consumers do not experience any constraints in their legitimate usage of the content⁸¹⁹. Thus far, content providers have failed to meet this challenge and consumers are frustrated by the restrictions placed on how they can use content they own. These frustrations are enough to encourage piracy. IDC⁸²⁰, an industry research firm, provides some insight into what constraints consumers are willing to accept for music files for example. The results are outlined in Figure 5.

It is important to note that the majority of individuals would not accept most of the constraints presented in Figure 5 and that these constraints are the weaknesses of current protection technologies (e.g., limited device range, usage tracking, inability to share). Therefore, for protection technologies to succeed in a Business-to-Consumer environment, their implementations must focus on flexibility, portability, usability, and privacy and content providers must focus on offering services that are customer centric.

⁸¹⁶ See: Yoon (2001); Orwat (2002).

⁸¹⁷ See: SIIA (2001).

⁸¹⁸ See: N.N. (2002).

⁸¹⁹ See: Pfeiffer (2001); Berry (2002).

⁸²⁰ See: IDC (2000b).

In the first section, this paper illustrated how the costs of copying an illegal copy depend on the strength of protection technologies and the degree of law enforcement. Protection technologies, such as encryption, watermarking or digital fingerprinting enable content providers to restrict, access, track, and locate individuals who behave illegally (e.g., download legally the content and distribute it illegally over peer-to-peer networks). But it is the responsibility of law enforcement agencies to punish these pirates and not the protection technologies or the content providers. So, despite the abilities the content providers now have through digital protection technologies, their effectiveness is bottlenecked by government enforcement bodies.

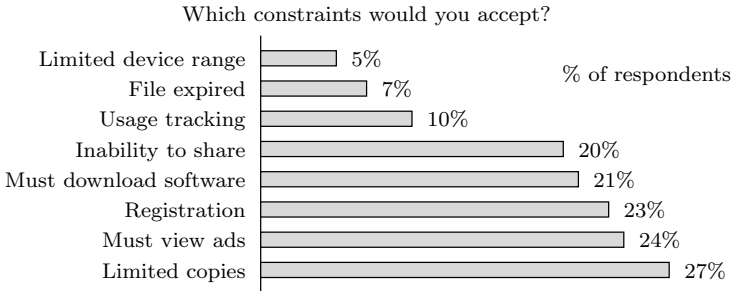


Fig. 5. Constraints Consumers Would Accept

Section one of this paper assumed that protection technologies do not restrict lawful consumers. However, as Figure 5 has shown, these technologies do restrict consumers in their usage of the legally acquired digital content. Therefore, the model must be expanded accordingly and recommendations about the consumer acceptance of protected digital content can be given.

An additional variable (φ) must be introduced into the model where $0 \leq \varphi \leq 1$ captures the degree to which protection technologies restrict individuals in the usage of the original. Let vp_i represent $vo_i(1 - \varphi)$ for the value perceived by individual i for the protected original. For example, when $\varphi > 0$, the protection technology is restricting the consumer and the perceived value of the protected original (vp_i) is smaller than the original without any protection technology (vo_i). If protection technology would not restrict the consumer ($\varphi = 0$) vo_i equals vp_i . Figure 1 presented four situations for an individual — either he is in an environment with a perceived weak or a perceived strong law enforcement and he may perceive the copy as a substitute or as an imperfect substitute in regards of the original.

$vo_i \hat{=}$ Perceived value the individual places on the original

$p \hat{=}$ The Price for the original

$vc_i \hat{=}$ Perceived value the individual places on the copy, $vo_i(1 - \delta)$

$\delta \hat{=}$ Captures the quality differential between the original and the copy

$x \hat{=}$ Expected fine ($x = \mu f$)

$vp_i \hat{=}$ Perceived value the individual places on the protected original,
 $vo_i(1 - \varphi)$
 $\varphi \hat{=}$ Amount of technology restriction faced by the lawful consumer

The following analysis is based on the model and framework presented in the first section of this paper.

Weak Law Enforcement

In an environment where an individual perceives a weak law enforcement (thus $x = 0$), the introduction of protection technology can be presented as follows. Taking equation (5) from section one of this paper, the following transformation is made to account for the introduction of protection technologies (i.e., usage restrictions).

$$\begin{aligned}
 vo_i - vc_i &\geq p && \text{(unprotected original)} && (5) \\
 vp_i - vc_i &\geq p && \text{(protected original)} && (7) \\
 \underbrace{vo_i(1 - \varphi)}_{\text{legal}} - \underbrace{vo_i(1 - \delta)}_{\text{illegal}} &\geq p && && (8)
 \end{aligned}$$

It is assumed that the illegal copy does not include any protection technology (i.e., if not it would not exist) and would not restrict the pirate in its usage. In addition, the illegal behavior would not be punished, thus $x = 0$. As the lawful consumer is restricted in his usage (e.g., number of devices limited), the perceived value of the protected original (vp_i) will be smaller than the original without any protection (vo_i).

From this two situations can be analyzed:

Situation ①: when $vo_i - vc_i = 0$, thus $p = 0$. When introducing protection technologies to protect the original, it would reduce the perceived value of the original by a factor φ . Therefore, when $vo_i - vc_i = 0$, and $vp_i < vo_i$, thus $vp_i < vc_i$ the consumer prefers the copy to the original.

Situation ②: when $vo_i - vc_i > 0$, thus $p > 0$. In this case, it depends on the gap between the unprotected original and the copy (e.g., $vo_i - vc_i > 0$,) and the amount of restriction the protection technology places on lawful consumers (φ). Introducing protection technology reduces the value of the original by a factor φ , thus $vp_i = vo_i(1 - \varphi)$. As equation (8) shows, the gap can be presented by $vo_i(1 - \varphi) - vo_i(1 - \delta) \geq 0$. Thus, as long as the degree of restricting the lawful consumer (φ) is smaller than the perceived quality difference between the original and the copy (δ), the consumer might accept protection technologies. In the other case, the consumer might prefer the copy.

Strong Law Enforcement

In an environment where an individual perceives a strong law enforcement (thus $x > 0$), the introduction of protection technology can be presented as follows. Taking equation (6) from section one of this paper, the following transformation

is made to account for the introduction of protection technologies (i.e., usage restrictions).

$$vo_i - vci \geq p - x \quad (\text{unprotected original}) \quad (6)$$

$$vp_i - vci \geq p - x \quad (\text{protected original}) \quad (9)$$

$$\underbrace{vo_i(1 - \varphi)}_{\text{legal}} - \underbrace{vo_i(1 - \delta)}_{\text{illegal}} \geq p - x \quad (10)$$

Again two situations can be analyzed:

Situation ③: If $vo_i - vci = 0$, thus $p = x$. In this case, the individual perceives the value of the copy as a substitute to the original. In addition, the price the legitimate consumer pays equals the costs (i.e., expected fine) to obtain the copy. When introducing protection technologies to protect the original, it would reduce the perceived value of the original by a factor φ . Therefore, when $vo_i - vci = 0$, and $vp_i < vo_i$, thus $vp_i < vci$. If p and x remain unchanged, the individual prefers the copy as it provides for the same costs (i.e., $p = x$) a higher value than the protected original (i.e., $vp_i < vo_i$, thus $vp_i < vci$).

Situation ④: If $vo_i - vci > 0$, individuals value the original more than the copy. In this case, it depends on the gap between the unprotected original and the copy (i.e., $vo_i - vci > 0$), the degree of restriction placed on lawful consumers (φ) and the degree of law enforcement ($x = \mu f$). However, this is the most likely case for where individuals would accept protection technologies for two reasons. First, the original is perceived higher than the copy and introducing protection technologies can be justified. Second, the perception of stronger law enforcement may frighten individuals to behave illegally ($x > 0$).

Figure 6 summarizes the possible consumer acceptance for protected digital content.

		Law Enforcement (costs)	
		Weak	Strong
Perceived value	Imperfect substitute $vo_i - vci > 0$	Might accept ②	Accept ④
	Substitute $vo_i - vci = 0$	Not accept ①	Not accept ③

Fig. 6. Consumer Acceptance for Protected Digital Content

This is not to suggest that protection of digital content is irrelevant. On the contrary, such barriers prevent a number of individuals from committing an illegal act, and make them aware that unintended use of the digital content is prohibited. However, this paper does argue that rethinking pricing (p) and

redesigning the value proposition to the individual (vo_i) of a digital content can contribute to reducing the illegal consumption. Ease of use (e.g., easy to find, download, use), perceived usefulness, and trust (e.g., payment system, privacy) are examples of what individuals require for legal acquisition of content⁸²¹. To compete, content providers must focus on making the original easier and cheaper to buy than to steal. The paradox with such protection technologies is that on one hand, content providers have to provide certain access to their valuable content in order to sell it, but on the other hand, must simultaneously try to restrict the consumer not to do everything with it⁸²².

It is important to note that to date individuals have rejected most protection technologies, including Digital Rights Management Systems. Let's take an example from the music industry where BMG released Natalie Imbruglia's new album, "White Lilies Island", in the UK with a copy protection scheme made by Midbar called Cactus Data Shield. Within a few weeks of the initial release, BMG was flooded by complaints that the CD was unplayable in some CD players. Numerous reports of unreadable first tracks, and incompatibility with personal computers forced BMG to reissue the CD without the copy protection and replace "defective" CDs upon request⁸²³. Again, this shows that instead of combating copyright infringement, these schemes harm legitimate consumers⁸²⁴. Arguably, this might be due to the introduction of new protection technologies — technical issues might be solved over time.

One good application for protection technologies is emerging when they are used not as a restricting tool but rather as a promotional tool (i.e., provide value to the individual). Again an example from the music industry. In June 2002 nearly two million Britons opened their Sunday edition of the London Times and found a free CD, from the band Oasis. It contained music and video tracks from the band's forthcoming album. It was distributed a week before the album's release. The CD allowed consumers to pre-listen to three of the album's new tracks on their personal computer. Fans were unable to copy the music files and post it to file-sharing systems. But, fans that wanted to hear more had to link to the band's web site and could preorder the new album from U.K. based retailer HMV or wait until the release. Preorders for the album exceeded company's expectations by 30,000 during the week following the Sunday edition of the London Times promotion. In addition, Oasis record company gained data from over 50,000 fans who registered online — new information that could be used to sell more CD's in the future. Finally, HMV was able to raise the number of visitors to its retail Web site, and even the newspapers homepage was able to score a win in the deal: Circulation that day was 300,000 its second-highest Sunday circulation ever⁸²⁵.

⁸²¹ See: Rosenblatt, Trippe, Mooney (2002); Thong, Hong, Tam (2002).

⁸²² See: Pfitzmann, Federrath, Kuhn (2002).

⁸²³ See: Triplett (2001).

⁸²⁴ See: Halderman (2002).

⁸²⁵ See: Marks (2002).

V Conclusion

Content providers have to view the Internet as a new and different distribution channel with its own consumer behavior, need and willingness to pay. They must come to understand that Internet piracy is here to stay and to learn how to compete against pirated versions of their own products. In addition, making individuals pay for digital content is a challenging task. The two most important factors, which content providers can directly influence, are the price and the value provided to the consumer. Therefore, content providers are better off investing time and effort in testing new pricing models and value propositions than the protection of their digital content. Moreover, content providers have to become aware of other factors, such as the distribution channel used, the consumer group, the type of content provided, and the cultural environment, that are all important drivers in an individual's willingness to pay. In general, protection technologies face consumer resistance and there seems to be only a few situations where consumers might accept its restrictions. Content providers have to carefully evaluate how and when to implement such technologies. They should also be aware of the impact of such technologies on the consumer behavior. For digital content distributed over the Internet, the highest consumer acceptance for protection technologies might be when they are used to promote the selling of digital content rather than the act of selling. However other situations may very well apply to digital content distributed over mobile networks, satellite, or television.

3.6 Lessons from Content–for–Free Distribution Channels

*Michel Clement*⁸²⁶

I Content for Free?

“If somebody comes to our service and is looking for a song and they can’t find it, the likely result is not going to be that they are going to turn off their computer, get in their car, drive to the record store and buy the CD. The likely result is they will now be forced off to a peer-to-peer site.”

Alan McGlade, CEO of MusicNet, interview given to CNET July 18, 2002

The most challenging task facing McGlade is licensing content for MusicNet, but the content he is looking for is already digitized, compressed, labeled, and widely published on the Internet. Peer-to-peer networks like KaZaA or iMesh virtually offer all content users desire. The only problem is that right owners did not license the content to them and users are acting illegal, if they offer content — and in some countries, when they download it.

A KPMG survey shows the currently favored strategies by media companies. Encryption is by far the most popular strategy to fight digital piracy⁸²⁷. The defensive strategy of protecting content from being copied and distributed by third parties is accompanied by heavy law enforcement to secure copyrights. Nevertheless the pure defensive strategy is wrong at this point of time, since it offers only short term relief. In the long run, users are getting more and more locked-in with peer-to-peer services. The economics of black markets do not make exceptions in the digital economy⁸²⁸. Without legal ways to access content, people will provide access to their content themselves and some of them will be able to monetize this market gap. Prohibition has always one loser: The customer.

The defensive strategy leads to a bumpy customer experience. For example the new “De Phazz”-Album “Daily Lama” is copy protected. The customer spends €15.99 for a CD and is not able to play the CD on the PC without using the obscure player that is included on the CD. It is not possible to play the CD using the standard Microsoft Media Player, which is installed on most PCs. At launch time a German customer was not able to download the new De Phazz songs from a legal source; even if he was willing to pay.

But customers can access the album plus a wide selection of other (related) content from a service, which is easy to use, offers great service without restrictions — and all this for free. This service is provided from the leading digital content distributor: KaZaA. The content industry does currently not offer any competitive download service.

⁸²⁶ University of Kiel.

⁸²⁷ See: KPMG (2002).

⁸²⁸ See: Givon, Mahajan, Muller (1995).

II Existing Distribution Channels

Media products are nothing else but information which can easily be digitized. On the one hand digital products have one major characteristic: they can be reproduced without loss of quality and with marginal costs of close to zero. On the other hand it is costly to produce the master copy, and labels, studios, or publishers try to secure their investments by using encryption methods usually embedded in DRM-Systems⁸²⁹. Using encryption methods raises the costs for pirates to produce their first master copy. But the potential reward for pirates is high: Hackers are gaining recognition from insiders, if they crack a new encryption method. But it is not necessary for a mainstream user to be a hacker to access encrypted content. It is sufficient, if one person in the world is willing to invest his time and money in producing the first master copy without encryption⁸³⁰. If this file is offered on KaZaA, in just hours the file will be spread over the world, assumed that demand is high.

Users create an important channel to digital content distribution⁸³¹, by adding value in a process that starts with digitizing and ends with distributing content (figure 1):

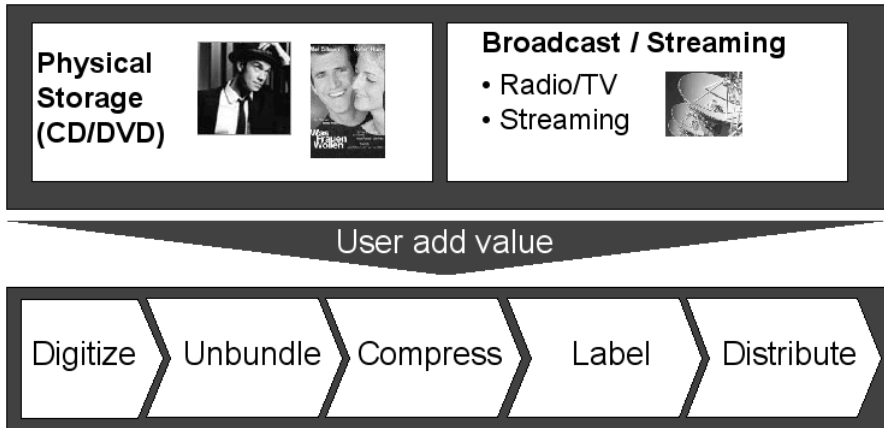


Fig. 1. The Piracy Value Chain of Users

Technology enables users to create a new master copy of basically any encrypted media product without being a professional computer scientist. The data source to produce the master copy comes either as a physical storage medium like a CD or DVD or via broadcast or streaming to the user. Ripping CDs is a standard application integrated in most MP3-Players and therefore mainstream, whereas the digitization of a DVD on a PC is a little more complex⁸³², but easy to use tools like “DivX Video Bundle” are becoming increasingly popular.

⁸²⁹ See: Durlacher (2001).

⁸³⁰ See: Hess, Anding, Schreiber (2002).

⁸³¹ See: Geyskens, Gielens, Dekimpe (2002).

If CDs (like De Phazz) with copy protection can not be ripped by using standard software like Windows Media Player, users look for alternatives. There are enough free software products out in the market (download.com) that offer the solution. Most of these products record digital audio tracks directly from compact discs, without going through the sound card (i.e. Freerip MP3 or Total Recorder).

Even if there is no chance to break the encryption from the digital source CD or DVD, there is always the final method to get the songs digitized on the PC: About 25 years ago kids were sitting in front of the family radio with a tape recorder waiting for the song to play in the radio. When the speaker announced the song to be played they pushed the record button. The same mechanism works today, but with more sophisticated technology. A home CD-Player can be connected to a PC using “audio in” and software products like “Cybercorder 2000” (US\$ 24.95; <http://skyhawktech.com>) will record from any sound input. Recordings are saved as WAV or MP3 files on the PC hard drive. The fact that media products always need an analogue display (sound for music, screen for videos, paper for pictures etc.) will allow recording and copying, regardless what encryption is used in the consumer market.

Media products are physically stored on CDs/DVDs or broadcasted via radio or television stations. Many PCs have a TV tuner card installed and are able to record TV shows, MTV music videos, or songs from cable radio stations directly to the hard drive. The former analogue video technology is leapfrogged by digital VCRs which are PCs with TV tuner cards or extra hardware devices like “Personal VCR” (PVR) from TiVo or ReplayTV. Once a TV show is recorded and stored on the hard drive, it can be modified and distributed by users, regardless if the recording has been done on the PC directly or on a PVR.

Once the data is recorded or ripped on the PC users unbundle the product in its entities. The unbundling process can be automated. Bitbop, a PVR for music, was offering such a service for streaming (figure 2). Bitbop scanned the radio program of internet radio stations and a user could enter a list of his most favorite artists. Bitbop searched the radio stations and automatically picked the best stations based on your favorite artists. The software connected to internet radio stations and automatically recorded songs, played by the favored artists. The files were stored on the user’s hard drive. Although the company suspended the service, others are just as useful: For example Streamripper, which is a tool that automatically rips each song streamed to Winamp in the MP3-format. All a user needs to do is to wait several hours and the complete radio stream is ripped in individual songs, compressed in MP3, and originally labeled on the hard drive.

A ripped CD is unbundled in each song and one specific TV show is recorded from the broadcast stream. Users cut the advertisements by using standard video software (i.e. David TV, www.tobit.com) and compress the TV show by using standard codecs. Compression technologies are important, because they reduce

⁸³² See: Hess, Anding, Schreiber (2002).

the size of the media file enormously. The standard codec for music is MP3 and for videos DivX;-), while Books are usually saved in PDF-formats. Media companies tried to influence hardware manufactures not to allow MP3 or DivX;-) files to be played on hardware devices, but market demand was too strong and manufactures could not resist. At the beginning it is usually a no-name manufacturer offering the first devices without limitations, but soon Philips and others are following: Portable music players that do not allow MP3-files to be played are not successful anymore. The movie industry is facing the same challenge, because users would love to play their burned CDs with DivX;-)-coded movies on their DVD-player; and manufacturers like Kiss Technologies and Yamakawa have already announced DVD players with DivX;-)-functionality.

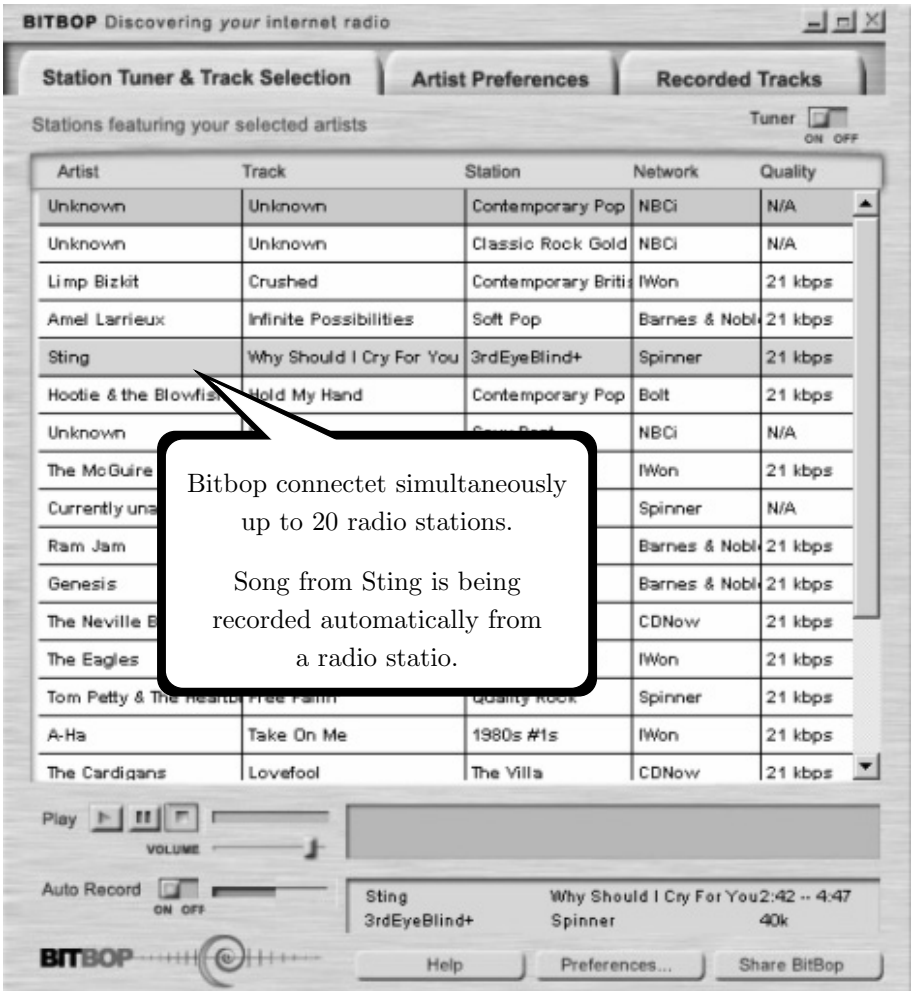


Fig. 2. Bitbop — Personal VCR for Streaming Audio
 Song Is Recorded automatically from a Radio Station

Once the data is digitized, unbundled, and compressed, users label the songs or movies themselves. They also provide the booklets. Sites like darktown.com offer scanned booklets to download. The offered booklets have the required size and with a color printer booklets can be printed by everybody. Even audio-book covers are available (figure 3):

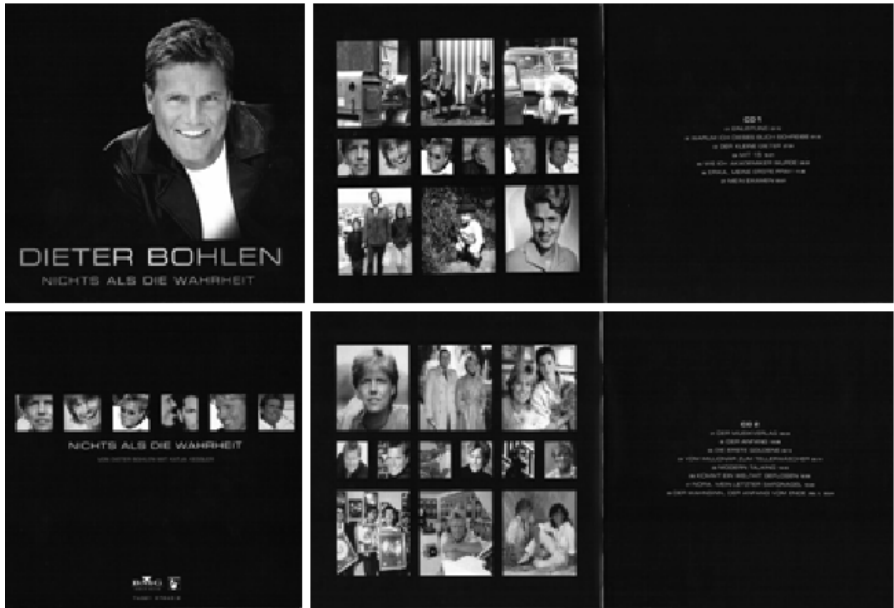


Fig. 3. Booklet from Dieter Bohlen’s Audio Book

Piracy is nothing new to the media industry, but with the rise of peer-to-peer pioneer Napster, a new “quality” of illegal mass distribution has been reached. The most important two services offered by filesharing networks are:

- indexing of files and
- peer-to-peer-connections.

A filesharing network primarily offers the information what files are offered by other users in the network. This information is stored in an index which is either centrally on the provider’s servers (i.e. iMesh) or decentrally (i.e. Gnutella, KaZaA) on the user’s machines. The search requests for files are directed to the index which returns the available files offered by other peers. With a double click on the demanded file the second service is offered: A direct connection to the peer allowing data transfer. Every day more than 3.5 million users are offering more than 600 million files at KaZaA and more than 500.000 movies are downloaded⁸³³.

⁸³³ See: Clement, Nerjes, Runte (2002); Detecon (2002).

But peer-to-peer is not only restricted to the PC. People with a ReplayTV Personal VCR can use planetreplay.com to exchange recorded TV shows (figure 4):

The screenshot shows the Planet Replay website interface. At the top, it says "Planet Replay" with the tagline "SOME OWNERS HAVE ALL THE FUN". Below the header, there's a navigation menu with "Quick Links" and "Welcome to Planet Replay v0.7". The main content area is titled "Planet Replay's Shared Shows" and includes a search bar with a "SEARCH" button. Below the search bar, there are four sections: "Most Recorded Shows", "Most Borrowed Shows", "Most Active Users", and "Most Active Users".

Most Recorded Shows

1. Friends
2. The Simpsons
3. Seinfeld
4. Buffy the Vampire Slayer
5. Enterprise
6. South Park
7. Stargate SG-1
8. Firefly
9. Batman
10. Will & Grace
11. The West Wing
12. CSI: Crime Scene Investigation
13. Survivor: Thailand
14. Scrubs
15. Alias
16. Curb Your Enthusiasm
17. John Doe
18. Smallville
19. Good Eats
20. The Sopranos

Most Borrowed Shows

1. Firefly
2. Enterprise
3. The Sopranos
4. Friends
5. Survivor: Thailand
6. The West Wing
7. Birds of Prey
8. Buffy the Vampire Slayer
9. Alias
10. Boomtown
11. ER
12. John Doe
13. The Amazing Race 3
14. Angel
15. CSI: Miami
16. Scrubs
17. Push, Nevada
18. CSI: Crime Scene Investigation
19. The Bachelor
20. Law & Order: Special Victims Unit

Most Active Users

1. Abb 4320	☆☆☆☆☆
2. plasmar	☆☆☆☆☆
3. scottsf5	☆☆☆☆☆
4. RSL	☆☆☆☆☆
5. roop3971	☆☆☆☆☆

Most Active Users

11. Amazingly Smooth	☆☆☆☆☆
12. Ice Pic	☆☆☆☆☆
13. WA6DZP	☆☆☆☆☆
14. Robbo	☆☆☆☆☆
15. Clark 858	☆☆☆☆☆

On the left side of the page, there's a sidebar with "Find a Show" search bar, "Discussion Forums", "ReplayTV Resources", and "Site Statistics". The "Site Statistics" section shows: Members - 955, Requests - 71, Shared - 12230.

Fig. 4. Planetreplay — Sharing Recorded TV Shows

Enforcing copyrights by law does not eliminate this peer-to-peer phenomenon. The end of Napster showed the flexibility and demand in the market. Millions of users searched for alternatives. Without competitive legal download sites they went to KaZaA, Gnutella, iMesh, etc. Some of the networks are open source (i.e. Gnutella, OpenNap) and some are designed for complete anonymity (i.e. Freenet 0.5). The media industry will therefore not be able to stop this technology anymore⁸³⁴.

But there are also other distribution channels in the market in addition to peer-to-peer: Years ago the Usenet was the prime source for media files. Software products like “Tifny” will automatically search user defined favorite Usenet newsgroups, identify the image and music files of interest, and download them. Instant messengers like AIM or ICQ offer peer-to-peer connections without indexing files, but peers can define upload directories that can be browsed by others — including data transfer.

Therefore it is no wonder that the new copy protected album from De Phazz is available for download at KaZaA.

⁸³⁴ See: Moon (2002).

III Locked-In User

The more penicillin the more resistant the virus.

Genie is out of the bottle. Users provide a majority of the value chain in the peer-to-peer world, develop the technology in open source projects, and offer access to their hard drives. The more legal action is being undertaken, the more the developers of peer-to-peer software will use open source or decentralized, anonymous distribution networks to secure the service from being legally stopped.

It is pure anarchy out in the market — and this anarchy develops good software products with customer suited services. The critical mass has long been reached and the guideline for successful innovations (Table 1) shows why the diffusion process of peer-to-peer software was the fastest ever seen⁸³⁵.

Roger's criteria are all fully satisfied and network externalities are high. Peer-to-peer networks are communication networks and therefore classical critical mass systems⁸³⁶. The more users in the network, the more content is available and the higher the utility⁸³⁷. But also indirect network externalities are heavily raising the utility — any question regarding problems with installation or downloads will be answered from the community on zeropiad.com and other tech-sites. In addition to the network externalities there are substantial word-of-mouth effects in the market⁸³⁸.

Online customers are choosing their distribution channels mainly because of technology reasons. The technology acceptance is a key factor in the choice and satisfaction of a B2C-distribution channel. It is determined by perceived ease of use and perceived usefulness of the channel⁸³⁹. Currently, both are very high in the illegal market, but low in the legal market.

Legal offers from MusicNet, PressPlay etc. use DRM to secure the content. The fact that users have to pay for content is only one issue that reduces the consumer surplus. This is only the case for users that do not perceive a higher value from accessing legal content. The other issue is the bumpy consumer experience. Using the Microsoft DRM allows content owners to differentiate each single content item with several business rules (Table 2).

Content owners have many possibilities to price each piece of content, depending on the rights attached to it. Currently a customer buys a CD and has all rights delivered with it. Some of the newer CDs come with copy protection and labels are heavily criticized for charging the same amount of money for fewer rights attached. The consumer experience is definitely not higher, if the song which was downloaded and paid for (1) expires after five plays, (2) can neither be backed up or transferred to another device, nor (3) burned on CD, to listen to it in the car etc.⁸⁴⁰. The constraint to renew licences will again lead the user to the payment

⁸³⁵ See: Rogers (1995); Tornatzky, Klein (1982).

⁸³⁶ See: Taylor (1994).

⁸³⁷ See: Brynjolfsson, Kemerer (1995); Graumann (1993).

⁸³⁸ See: Goldenberg, Libai, Muller (2001); Mahajan, Muller, Kerin (1984).

⁸³⁹ See: Devaraj, Fan, Kohli (2002).

procedure — a problem which is also not solved properly, because many young customers do not have credit cards and are not allowed to charge the music costs on the phone bill (popfile.de).

Criteria	KaZaA
Relative Advantage	<ul style="list-style-type: none"> • All content is available. No matter what label, what format, what kind of media. • Easy installation. • Easy navigation. • New albums are available months before the official release. Robby Williams' album "Escapology" was available at KaZaA two months before the launch. • Free service.
Compatibility	<ul style="list-style-type: none"> • The files are offered in the de facto standards MP3, DivX;-) etc. Therefore no compatibility problems arise. • High coolness factor — high compatibility in the social system.
Complexity	<ul style="list-style-type: none"> • Very low complexity. • Integrated media player does not require multiple updates for new formats • Play all files without limitations (duration, burning, transfer etc.)
Trialability	<ul style="list-style-type: none"> • Software is available for free. • Software products for Windows, Mac and Linux are available. • Great community to ask for help.
Observability	<ul style="list-style-type: none"> • Lot of press coverage through Napster and the "battle" against the RIAA. • Easy message: "Get all files".

Tab. 1. Drivers of successful Innovations

Some users feel that the offered services in the market are guided by the general technological design assumption of Microsoft's DRM: "The User is Untrusted". How do these services want to compete against free and illegal offers?

Networks like KaZaA offer more and more services to lock-in users and to prevent them from defecting to another service. User ratings, content ratings, playlists, web search etc. are included to add value and raise switching costs⁸⁴¹. Product line breadth is one of the most important factors to build up switching costs — something legal competitors like MusicNet struggle with⁸⁴².

⁸⁴⁰ See: Durlacher (2001).

⁸⁴¹ See: Patalong (2002).

⁸⁴² See: Chen, Hott (2002).

MS-DRM	Example of customer experience
Expiration After first Use	This business rule specifies the length of time (in hours) a license is valid after the first time the license is used. The content seller can set a license to expire 24 hours after a consumer begins to play the Windows Media file.
Expiration On Store	This right specifies the length of time (in hours) a license is valid after the first time the license is stored on the consumer's computer. The content seller can set a license to expire 72 hours after it is stored.
Allow Saving of Protected Streams	If a packaged Windows Media file is streamed, this right allows the consumer to save the stream as a file. The saved file remains packaged and still requires a license.
Player Application Exclusion	Player exclusion is a feature that allows a license issuer to prevent specific player applications from playing certain packaged files. The result is that consumers cannot play the packaged file on the excluded player application.
Allow Play On PC	Allows the consumer to play the file on a computer.
Play Count	Specifies the number of times a file can be played.
Allow Burn To CD	Allows the file to be copied to a CD in an unprotected format.
Burn To CD Count	Specifies the number of times a file can be copied to a CD.
Allow Backup Restore	Allows the consumer to back up licenses and restore them to the same computer or to different computers.
Begin Date	Specifies a date after which the license is valid.
Expiration Date	Specifies a date after which the license is no longer valid.
Delete On Clock Rollback	Deletes the license if the consumer resets their computer clock to an earlier time.

Disable On Clock Rollback	Disables the license if the consumer resets their computer clock to an earlier time, and enables the license once the clock is corrected.
Allow Transfer To Non SDMI	Allows the consumer to transfer the file to a non-SDMI-compliant portable device.
Allow Transfer To SDMI	Allows the consumer to transfer the file to an SDMI-compliant portable device. When using this right, the SDMI specification located on the Secure Digital Music Initiative Web site must be followed (http://www.sdmi.org).
Transfer Count	Specifies the number of times a consumer can transfer a file to a portable device.
PM Rights	Specifies the rights to give with portable licenses for this file. A portable license is a new license that accompanies a file when it is transferred.
PM Expiration Date	Specifies a date when a portable license expires.
Minimum App Security	Specifies the minimum security level that is required of a player application.
PM App Security	Specifies the minimum security level that is required of a portable device.

Tab. 2. Business Rules⁸⁴³

It can be premised that there are two segments of users: The innovators and the followers⁸⁴⁴. The innovators are using new technologies to download media files regardless whether they are legally offered or not. Innovators tend to be driven by their wish to lead the market whereas followers are influenced by the bandwagon effect and wait to adopt new technologies until the critical mass of adopters is reached⁸⁴⁵. Unlike May and Singer⁸⁴⁶ argue, it is absolutely clear that peer-to-peer technology is not used only by innovators anymore.

The longer it takes until the media industry will provide an offer, which is as simple as KaZaA, the higher will be the switching costs for the users. Additionally, they are getting used to the fact that content is for free, which will reduce the long term willingness to pay dramatically.

⁸⁴³ Source:

<http://www.microsoft.com/windows/windowsmedia/wm7/drm/newin7.asp#rules> and <http://msdn.microsoft.com/msdnmag/issues/01/12/DRM/default.aspx>.

⁸⁴⁴ See: Bass (1969); Mahajan, Muller, Bass (1990).

⁸⁴⁵ See: Moe, Fader (2002).

⁸⁴⁶ See: May, Singer (2001).

IV Unlocking User to Customers

Media companies should put less emphasis on protecting their content from digital distribution. Instead they should identify ways to make money from selling music, movies or books online to beat pirates on their own terrain.

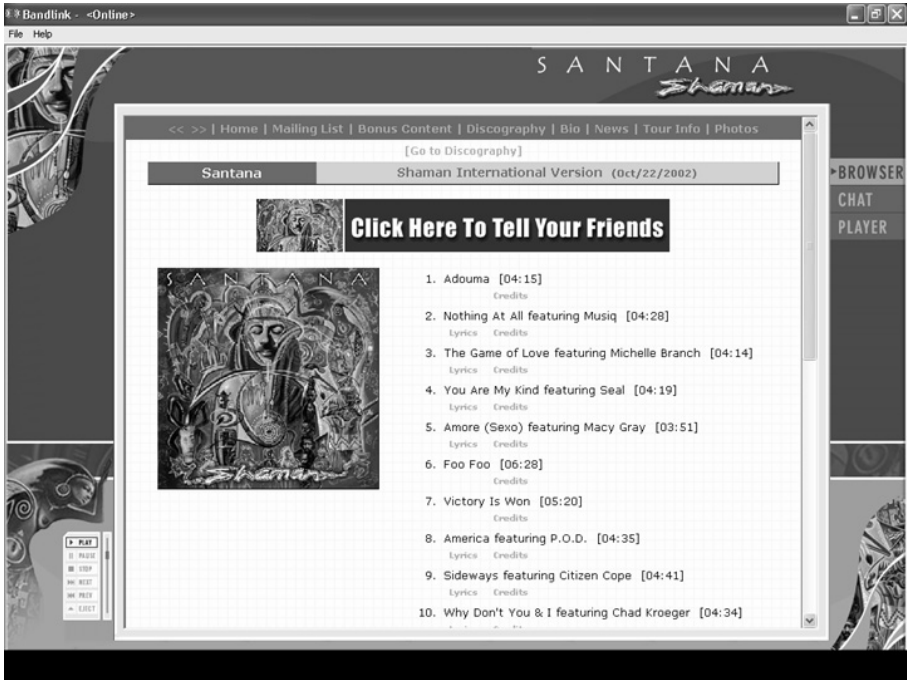


Fig. 5. Santana and Bandlink

Filesharing and all the other illegal distribution channels exist, because the market wants them — the demand creates its supply. In 1996 David Bowie made his single “Telling Lies” available for download, free of charge and for one week. In that week the single was downloaded 450,000 times from fans in more than 80 countries⁸⁴⁷. But in 2002 still only 43% of the media companies are making their content available in digital form⁸⁴⁸. The fear of channel conflicts and cannibalization of sales through the online channel is sometimes too high for labels to license their content for online distribution⁸⁴⁹. This shows that the media industry favors the defensive strategy — leaving pirates to satisfy the market demand.

⁸⁴⁷ See: Krasilovsky, Shemel (2000): 447.

⁸⁴⁸ See: KPMG (2002).

⁸⁴⁹ See: Harmon (2002).

Few media companies are using an offensive strategy. Some of the newer services are putting more emphasis on consumer experience. Universal Music's German service Popfile.de is a good example.

The best example of using an offensive strategy is the new album of Santana "Shaman", which is sold for €12.99. The CD is not copy protected but enhanced with "Bandlink", a software that offers community services, access to additional content like lyrics, biography etc. Users that insert the CD in their PC are guided to the Bandlink software which starts right away with a window where lyrics and credits are presented (figure 5).

The user has many features and can access bonus content from Santana. Videos, promotions, unpublished songs, photos etc. (figure 6).

In addition to these enhanced services, the user can access a Santana chat community. This community is joined by other Santana fans worldwide that are listening to the CD on their PC (figure 7). Users can even see what tracks chat partners are currently listening to.

The Santana album is a very good example in giving the user more value without withholding rights: The CD is not copy protected. Of course users of KaZaA can download Santana songs, but without the CD their fun is limited.

The analysis in this paper shows that DRM is mostly misunderstood by the content owners. Microsoft, Intertrust and others are providing DRM technology which allows a variety of restrictions and pricing models. The content industry sees the chance to not only protect the content, but to gain back control over the distribution and usage of content by users.

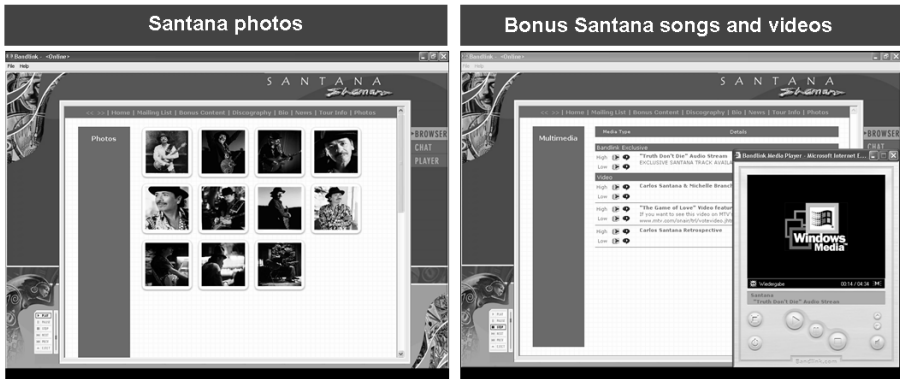


Fig. 6. Santana Bonus Content

But, DRM is about managing rights — Labels and artists want to get back more control over the content and over the customer⁸⁵⁰. The customers are spoiled by free alternatives and are not willing to give away their freedom in using content as they did before. All content is easily available online — provided by pirates⁸⁵¹.

⁸⁵⁰ See: Harmon (2002).

⁸⁵¹ See: May, Singer (2001).

The only thing which is hard to get, is legal content (which comes with many restrictions). As Slive and Bernhardt⁸⁵² argue, piracy can be viewed as a form of price discrimination in which the content provider sells some items for the price of zero. In this case it may help to promote the media products.

If the content industry targets late adopters of media download services that are not locked in yet, they might be able to position a service. But, if this service is not easy to use, without the necessity to install new players (to play the DRM files), and with unlimited use than even the late adopters will adopt KaZaA — for free.

Or, as the Wall Street Journal Europe notes: “AOL, which was supposed to be MusicNet’s biggest distribution partner, informed Mr. McGlade early this year that it wouldn’t sell the service until he made it more attractive for customers. In a six-week trial, the internet giant’s test audience found that MusicNet was difficult to use, and complained about the limited selection of music and lack of portability”⁸⁵³.



Fig. 7. Santana Chat Rooms

⁸⁵² See: Slive, Bernhardt (1998).

⁸⁵³ See: WSJE (2002).

3.7 Standardization in DRM — Trends and Recommendations⁸⁵⁴

*Oliver Bremer*⁸⁵⁵, *Willms Buhse*⁸⁵⁶

I Introduction

Digital Rights Management (DRM) is one of the most heavily debated technologies currently. Several attempts are being undertaken to introduce DRM technology into mainstream products. Despised by consumers who fear for their right to fair use, e.g. enabling back-up copies for personal use, it seems to be considered a necessity for a profitable content business in the digital age by many content providers. Its benefits, drawbacks and even implications to society itself are fiercely debated among and between consumer advocates, media power houses, governments, consumer electronics (CE) industry, IT vendors, service providers, and individual consumers alike. The very nature of DRM and the conflicting opinions of consumers and content providers surrounding it make it an extremely difficult topic to constructively discuss, let alone agreeing on.

Technology standardization, on the other hand, is a process characterized by reaching industry consensus. A significant number of interested parties with varying backgrounds collaborate in standardization in order to define technologies that serve the interests of the entire group. In short, technology standardization is a consensus driven activity for the common good.

DRM seems to be a perfect case study for standardization. In this paper, we analyze the effects of standardization of DRM. We first take a look at standardization in general, its purpose and functions, and its relation to patents. We then discuss a particular case of DRM standardization by using the example of the Open Mobile Alliance (OMA).

In the OMA, a multitude of different stakeholders such as operators, handset manufacturers, technology and content providers work together to meet the requirements from participants of the various content businesses.

We set out to illustrate that the technology to enable a successful deployment of Digital Rights Management for real-world implementations is best developed in an open standardization forum.

II Standardization

II.1 Framework and Definition

Standardization itself is a well known concept. Ever since industrialization began, standards of one form or another came into existence. With the ability of

⁸⁵⁴ Note: The views and opinions presented in this article are those of the authors and not necessarily of the organizations that employ them.

⁸⁵⁵ Nokia.

⁸⁵⁶ Bertelsmann Digital World Services.

producing goods in great quantities came the possibility of tapping into huge markets with decreasing costs. Standards at the very early stages were often of de-facto nature, i.e., created by market force through a single or few stakeholders. With a growing number of parties being able to meet the demands of the markets, joint standardization became a more open means of further growing the market and then sharing the benefits among multiple suppliers. Standardization, both open and de-facto, has retained its importance also in today's high tech markets. While open standards are used to jointly grow markets, they also enable a multi-vendor environment which in turn can be employed to limit the extent to which a dominant player in one market can exert its superior position to break into and control new markets.

Despite its long history, no single definition of standardization has been adopted. One could state that the notion of standardization itself has resisted 'standardization'. It is for that reason that we present different definitions of standardization.

Germon defines standards from a socio-economic perspective as a construct that results from reasoned, collective choice and enables agreement on solutions of recurrent problems. It can be understood as striking a balance between requirements of the involved parties, the technological possibilities and associated costs of producers, and constraints imposed by governments for the benefit of society in general.⁸⁵⁷

From a technical point of view, an industry standard represents a set of specifications, to which all elements of products, processes, formats or procedures under its jurisdiction must conform. The process of standardization is the pursuit of this conformity, with the objective of increasing the efficiency of economic activity.⁸⁵⁸

According to a recent definition by the EU, open standards must be consensus-based — involving all stakeholders, including consumer organization representatives — publicly available, transparently agreed, and commercially exploitable on a fair and non-discriminatory basis. The development of standards must therefore take the public interest into account, while standards themselves can play an important role in supporting public policy, and in providing tools for industry to meet regulatory requirements, or take account of public interest issues.⁸⁵⁹

As can easily be seen, the definitions above are related by similar underlying concepts yet they have divergent characteristics when it comes to the exact scope of standardization.

In this paper, we define *technology standardization* as a process taking into account requirements from multiple stakeholders in the value chain of the market for which the technology is determined resulting in a set of technical specifications potentially accompanied by IP licensing requirements enabling real-world implementations.

⁸⁵⁷ See: Germon (1986).

⁸⁵⁸ See: Tassej (2000).

⁸⁵⁹ See: CEN/ISSS (2003).

Open technology standardization extends the above definition by requiring stakeholders from the entire value chain to be able to jointly and equally collaborate in scoping, defining, developing and governing technical specifications enabling real-world multi-vendor implementations as well as conducting interoperability testing of implementations based on the specifications which are made publicly available.

The success of a standard, either de-facto or open, is ultimately measured by its interoperable adoption of stakeholders and its penetration in relevant markets. Achieving interoperability within a standard eliminates levels of complexity in implementing limited or partial standards. With interoperability among system components, such a market retains advantage of diversification at the component level, but also achieves the efficiency advantages of interoperability.

II.2 Purpose and Function

The importance of technology standards has risen for several reasons. An especially significant role in the area of high-tech standards is played by an ever faster development and replacement of technology paired with the constantly growing complexity of products entering mainstream markets.

Over a technology's life cycle standardization can affect economic efficiency — both positively and negatively. Several competing standards — either locally or industry segment-specific — can coexist for some time, but will be resulting in complaints about inefficiency. In mobile networks, e.g., for GSM, more coordinated efforts were undertaken in order to gain first mover advantages especially in the EU, which resulted in technology leadership in the EU compared to the US.

The function of standards and their purposes can partially be derived from the above definitions. Standards can be perceived as serving several purposes. The following characteristics describe the functions of standards:⁸⁶⁰

- *Quality and reliability*: specify acceptable performance and behavior such as functional levels, security, robustness, scalability
- *Information*: provide common languages such as engineering information, dictionaries, describing and testing, even product attributes
- *Compatibility and interoperability*: specify properties that a product must have in order to work with complimentary products within a system. This can be achieved through standardized interfaces between components and protocols
- *Variety reduction*: standards limit the choice to attain economies of scale. This applies to data formats, Meta data, algorithms, and architectures. Naturally, with high economies of scale involved, the involved companies tend to grow to large companies in this process

As already mentioned above, standards are used to jointly grow markets for whose shares the participating parties compete later on. Open standards enabling multi-vendor implementations can also be used as a tool to limiting the

⁸⁶⁰ See: Tassej (2000).

extent to which a dominant player can exert its superior position to break into and control new markets.

The more distributed the participants in the market, the more critical to technological innovation are open systems. Open standardization creates multi-lateral governance, thus promoting a multi-vendor environment by preventing a single company from changing the standard to render its competitors' products incompatible. The advantage of open governance can only be stifled by patents.

II.3 Innovations and Patents

Today, patents are an integral part of technology creation and development. Introduced centuries ago aimed at spurring innovation and information sharing, they are an important tool to protect intellectual property. They reward those who made the investment in R&D (Research and Development) ultimately leading to new ideas and technology. However, opinions on the benefit and usefulness of patents are split. There are two diverging schools of thought.

- The first group believes that patents stifle competition. The process of applying and finally being granted a patent can be lengthy and costly, especially for the budget of smaller companies. Big corporations usually hold the biggest patent portfolios. IBM, for example, has been leading the list of companies with most patents granted per year.⁸⁶¹
- The second group advocates the innovation fostering aspect of patenting novel ideas and inventions. IBM, for example, is granted a high number of patents not due to being a big corporation, but because, every year it invests a significant amount of their resources into R&D.

Products based on new ideas that are protected by patents usually reach the consumer faster than those for which the manufacturer has no assurance that he will be faced by imitator competition soon after. As such, patents form an integral part of assuring any company that it will be able to recover its investment into R&D by selling products based on the results of that R&D activity. Without assurance of return of investment (ROI), companies might not make this investment in the first place.

The impact of patents on standards depends on the nature of the resulting standard, i.e., whether it is proprietary or open.

In the case of a single company trying to establish a proprietary product as the de facto standard, patents can be used to hinder competition by not licensing the patent to the manufacturer of a competing product, whether it is proprietary or according to an open standard. However, it is seldom the case that a single company holds all essential patents to a technology. Thus, it is unlikely that a single company suffocates all competition on the grounds of patents because it could be subject to the same practices by another company, resulting in a lose-lose situation. Large corporations sometimes form strategic relationships and agree on cross licensing of patents in their respective portfolios to create

⁸⁶¹ See: IBM (2002).

win–win solutions where the participating companies are able to enter the market and compete, e.g., with technical features of their products.

Open standards bodies often require participating companies to declare their intellectual property that relates to the technology being standardized. This provides the advantage of all companies being mutually aware of the patents held by other companies participating in the standardization process.

III Digital Rights Management

III.1 Standardization — Perspectives

DRM is a very dynamic technology that is still in its infancy in terms of market penetration. While first patents in the field of DRM date back to the late 80s, the first standardization efforts in the field of DRM were started about 10 years later. Today, many standardization efforts related to DRM can be found. Lyon⁸⁶² enumerates in his quick reference list of organizations and standards for DRM more than 60 efforts. In the past, this has led to market segmentation in those areas and to confusion along the value chain.

The main reason for this segmentation can be found in the fact that requirements for DRM standardization vary across distribution channels and end devices. E.g. patient information has different security requirements than entertainment content. Additionally, also content providers from verticals like games, music, film or publishing have different views on the requirements to DRM to enable their respective businesses.

Still, DRM is a fascinating case study of standardization. It involves at its broadest consumer adoption, complex technological processes, varying requirements from a multitude of players in the value chain, while at the same time carefully balancing consumer experience and security requirements. Digital rights management and standardization thereof affect several parties with different benefits.

From the *content provider* perspective, which refers to the rights holder as well as to the distributor, standardization allows for the existence of several technology providers. With a broad supplier selection the technology costs for critical components are lower when compared to a market dominated by a monopolistic provider. Also switching costs are lowered and one–time hosting and packaging costs are lower compared to increased content–related costs for several non–standardized providers, while performance is optimized. The protected content market is still very immature while different business models are still being explored. In this situation, the flexibility provided through open standards where components can be replaced as the innovation progresses seems to be the beneficial approach for content providers. An overall consumer demand aggregation will also lead to network effects and increasing returns for protected content. Still content providers fear negative lock–in effects of any single dominant, proprietary DRM technology supplier.

⁸⁶² See: Lyon (2002).

Looking at the *DRM supplier* perspective, standards in DRM can create bigger markets by earlier consumer adoption based on rapid technology penetration. Provided open standards are in place, it allows for continuous technology upgrades on both sides of standardized interfaces and thereby creating an innovation-friendly environment. In case of a de-facto standard in DRM, it might result in one dominant technology provider, while other providers will be pushed into market niches and potentially vanish over time.

From the *hardware manufacturer* perspective providing client devices (PCs, mobile phones, set-top boxes, etc.), standardization lowers the manufacturing costs and risk by advertising lock-in to a single technology provider. The requirement for interoperability testing in a multi-vendor environment is a small price to pay compared to the market not taking off altogether or leaving it open to proprietary technology vendors. Ultimately manufacturers benefit from substantial economies of scale in production fostered by adoption of a single (that is standardized) DRM technology.

The consumer ultimately benefits from an increased selection of valuable content previously not having been available for purchase as electronic media. Additionally, interoperability between different device categories adds to the positive end user experience and the ease of use by being able to legally consume and share protected content with a number of different devices.

Different approaches can be applied to standardization of DRM.

- Only the interfaces between different components in the back-end, on clients and between these two are specified. This leaves actual design and implementation of the internal functioning of these components up to individual manufacturers.
- Not only the interfaces, but also the behaviour of the different components themselves is specified. In DRM, this is, for example, the protocols between clients and back-end used to acquire content and rights, the format of the secure package that protects content, and the rights governing the usage of content.
- Not only the interfaces and the behaviour of different components, but also their exact internal implementation is specified.

De-facto standards based on proprietary technology are usually of the third kind since actual implementations must be available for manufacturers of clients and operators of back-ends to put a working system in place. Often, standardization bodies adopt one of the former two approaches. This yields situations where individual suppliers develop their own components that interoperate via the standardized interfaces. In section *Open Mobile Alliance DRM*, we will have a closer look at a standardization forum following the second approach.

Moreover, in earlier markets, as can be observed with Internet-based DRM starting in 1998 and with mobile DRM starting in 2002, companies offer turnkey or end-to-end solutions where proprietary interfaces link components. In these cases, limited price competition through lock-in situations can be observed.

An effective design of an interface standard does not affect the design of the component itself. It provides open systems, allowing multiple proprietary component designs to coexist. With regard to DRM, these closed, proprietary components gain importance when it comes to security as encryption keys and other secrets have to be hidden within those components. Still, innovation can happen, allowing components from different parties working together and even the substitution of more advanced components as they become available over time. This greatly reduces the risk of obsolescence of the entire system also when it comes to security threats.

III.2 Open Mobile Alliance DRM

The Open Mobile Alliance (OMA) was formed in June 2002 through consolidation of the Open Mobile Architecture initiative and the WAP Forum. Since then, the Location Interoperability Forum (LIF), SyncML, MMS Interoperability Group (MMS-IOP), Wireless Village, and the Mobile Gaming Interoperability Forum (MGIF) have integrated into the OMA. The OMA counts more than 300 companies as its members.⁸⁶³ Members of the OMA include operators such as 3, AT&T Wireless, NTT Docomo, Orange, T-Mobile, Vodafone, hand set manufacturers such as Motorola, Nokia, Samsung, Siemens, Sony-Ericsson, and technology providers such as Ericsson, IBM, Microsoft, Philips, Real Networks, Sony, Sun, DRM providers such as Digital World Services, Lockstream, SDC, and content providers such as Disney and others.

The OMA is uniquely positioned to develop an open standard for Digital Rights Management. It enjoys the participation of a multitude of players in the value chain, many of which are key players in a flourishing content market. Already in 2001, the sale of content in the mobile world in Europe was more than double of that in the wireless world.⁸⁶⁴ The Open Mobile Alliance has already released a set of three specifications constituting the world's first DRM standard targeted at mobile devices. This first release, commonly referred to as *OMA DRM release 1*, defines multiple components of a DRM system. These components comprise

- the secure format through which content in the OMA DRM system is protected
- rights according to which content may be rendered by client devices
- protocols for transferring content and rights from network servers to client devices

The approach taken by the OMA makes it an instance of the latter of the two approaches described in section III. It not only specifies the interfaces but also goes so far to define the behaviour of components themselves. As such, DRM as standardized by the OMA provides the advantages of open standardization (section II) while at the same time enabling manufacturers of clients and operators of back-end services to immediately deploy a system based on this standard.

⁸⁶³ See: OMA (2003).

⁸⁶⁴ See: Jupiter Research (2002a).

The OMA also provides many of the functions of open standards such as enabling market growth, compatibility and interoperability (see section *Purpose and Function*). Stakeholders from the entire value chain coming together in the OMA jointly grow the global market based on an open standard framework permitting the efficient and reliable development and deployment of applications and services in a multi-vendor environment.⁸⁶⁵ The DRM developed by the OMA benefits from these functions of open standardization that are provided by the OMA.

The DRM architecture defined by the OMA enables super distribution of DRM protected content combining viral distribution of content known in a peer-to-peer fashion, yet retaining full control for content owners to allow and disallow consumption of the distributed content. This architecture explicitly allows for both centralized deployment, where there is a strong association between presentation server and download server, as well as decentralized deployment where there is a relatively low level of integration between presentation and download servers. The functionality enables the implementation of confirmed and reliable, and thus billable, transactions between a server entity (Presentation Server, Download Server) and a client device. The functionality allows any type of content to be delivered over any type of bearer to applications residing on clients independent of the operating system, thus fully conforming to the principles of the OMA.⁸⁶⁶

Through its rigid IPR policy, the OMA fully acknowledges the importance of patents. The IPR policy of the OMA is based on reasonable and non-discriminatory terms (RAND). It thus protects each member company's continued investment into R&D by ensuring proper licensing of patents for those member companies whose technology becomes part of a standard. At the same time, it ensures fair licensing of patents to its members in order to provide a leveled playing field in which one member cannot refuse licensing its IPR in order to stifle competition. Furthermore, it provides assurance to participating companies through the requirement for member companies to declare essential IPR that they are aware of regarding the technology being standardized.

The success of standardizing DRM in the OMA gains further credibility through the consolidation that has already taken place in mobile standardization efforts. Before June 2002, there were, among others, the WAP Forum and 3GPP. Since the consolidation of the WAP Forum and the Open Mobile Architecture initiative into the OMA, the interests of many players with respect to DRM have come together in the OMA. Also, the 3rd Generation Partnership Project (3GPP) have input their requirements for DRM to the OMA further consolidating the efforts for an openly governed DRM standard.

Therefore, OMA can be considered as a good example for the consolidation of DRM standardization within a specific industry. Additionally, OMA tries to establish liaisons with other related standardization efforts in order to create

⁸⁶⁵ See: OMA (2003).

⁸⁶⁶ See: OMA (2003).

synergies and in order to bring all value chain partners on board, including content companies from different verticals and from respective consumer groups

IV Discussion and Conclusions

Although various technologies for DRM have existed for quite some time now, it is at a relatively early stage in its life cycle. Not a single one of the proprietary solutions available to date has managed to establish itself as the de-facto standard for DRM in the market place. It could be argued that the market window has not opened up earlier and is currently about to provide the opportunity for a technology to separate itself from the rest of the field to become the de-facto DRM standard. While this is likely to have contributed to the current state of DRM, we argue that no single technology has emerged as the dominant DRM system due to the lack of an openly conducted standardization effort investing the time and resources in the development of a DRM standard.

The standardization of DRM is of particular interest since the flurry of high-tech start-ups creating a myriad of patents along the way. While many of these companies might be gone by now, the patents still exist somewhere, most likely as part of the patent portfolios of the companies that bought these start-ups. The patents generated by the start-ups, might very well be used by their new owners to prevent competitors from entering their market with DRM enabled products. The irony is that DRM — the technology aiming to protect intellectual property — might very well be hindered from taking-off by the intellectual property protecting the technology itself. Furthermore, DRM is a technology that effects a large number of stakeholders in the content business value chain without whose participation any DRM effort is doomed to failure. Especially, the perception that DRM has in the eye of the consumer make it a very difficult technology to introduce to the market.

We have demonstrated that the Open Mobile Alliance provides many of the advantages inherent to the joint development of technology through open standards. Moreover, the DRM effort conducted by the OMA is in the unique position to capitalize on the benefits that its vast range of member companies throughout the entire value chain contribute. In addition, the mobile market, already flourishing and surpassing that of the wireline Internet,⁸⁶⁷ proves to be the ideal catalyst for the successful take-off of a commercially deployed real-world implementation of DRM. With the arrival of high bandwidth wireless connectivity, the promise of new services comes one step closer to reality. Content providers, device manufacturers, operators, IT vendors and consumers alike, will not be able to benefit from this new opportunity without the proper content to give life to these services. Whether it is a ringing tone, the latest in mobile gaming, today's number one hit in the charts, or a video clip of the decisive moment in a sports match, the content, and thus the great new services themselves, are unlikely to materialize without the proper insurances for all players in the value

⁸⁶⁷ See: Jupiter Research (2002a).

chain on their return of investment. The Open Mobile Alliance Digital Rights Management effort is well positioned to provide the protection for this very content.

As mentioned above, there are many standardization efforts for DRM across different industries. Ironically, this market segmentation has brought more DRM-related standardization efforts than DRM technology providers. In order to build on the promise open standardization of DRM provides, the authors strongly recommend all industry participants to

1. work towards consolidation within their industries,
2. create liaisons with other such consolidated efforts and
3. motivate all value chain participants to provide input to the respective standards.

Ultimately, this will contribute to establishing a global DRM infrastructure in an open multi-vendor environment in which all stakeholders have their interests represented.

3.8 The Darknet and the Future of Content Protection

*Peter Biddle, Paul England, Marcus Peinado, Bryan Willman*⁸⁶⁸

Abstract: We investigate the darknet — a collection of networks and technologies used to share digital content. The darknet is not a separate physical network but an application and protocol layer riding on existing networks. Examples of darknets are peer to peer file sharing, CD and DVD copying, and key or password sharing on email and newsgroups. The last few years have seen vast increases in the darknet’s aggregate bandwidth, reliability, usability, size of shared library, and availability of search engines. In this paper we categorize and analyze existing and future darknets, from both the technical and legal perspectives. We speculate that there will continue to be setbacks to the effectiveness of the darknet as a distribution mechanism, but ultimately the darknet genie will not be put back into the bottle. In view of this hypothesis, we examine the relevance of content protection and content distribution architectures.

I Introduction

People have always copied things. In the past, most items of value were physical objects. Patent law and economies of scale meant that small scale copying of physical objects was usually uneconomic, and large scale copying (if it infringed) was stoppable using policemen and courts. Today, things of value are increasingly less tangible: often they are just bits and bytes or can be accurately represented as bits and bytes. The widespread deployment of packet switched networks, and the huge advances in computers and codec technologies, have made it feasible (and indeed attractive) to deliver such digital works over the Internet. This presents great opportunities and great challenges. The opportunity is low cost delivery of personalized, high quality content. The challenge is that such content can be distributed illegally. Copyright law governs the legality of copying and distribution of such valuable data, but copyright protection is increasingly strained in a world of programmable computers and high speed networks.

For example, consider the staggering burst of creativity by authors of computer programs that are designed to share audio files. This was popularized by Scour and Napster, but today several popular applications and services offer similar capabilities. In addition, CD-writers have become mainstream, and DVD-writers may well follow suit. Hence, even in the absence of network connectivity, the opportunity for low cost, large scale file sharing exists.

I.1 The Darknet

Throughout this paper, we will call the relevant items (e.g. software programs, songs, movies, books, etc.) objects. We will use the term to copy to refer to the duplication of objects in circumvention of copyright. The persons who copy ob-

⁸⁶⁸ Microsoft Corporation.

jects will be called users of the darknet, and the computers used to copy objects will be called hosts. The idea of the darknet is based upon three assumptions:

1. Any widely distributed object will be available to a fraction of users in a form that permits copying.
2. Users will copy objects if it is possible and interesting to do so.
3. Users are connected by high bandwidth channels.

The darknet is the distribution network that emerges from the injection of objects according to assumption 1 and the distribution of those objects according to assumptions 2 and 3.

One implication of the first assumption is that any content protection system will leak popular or valuable content into the darknet, because some fraction of users — possibly experts — will overcome any copy prevention mechanism or because the object will enter the darknet before copy protection is applied.

The term “widely distributed” is intended to capture the notion of mass market distribution of objects to thousands or millions of practically anonymous users. This is in contrast to the protection of military, industrial, or personal secrets, which are typically not widely distributed and are not the focus of this paper.

Like other networks, the darknet can be modeled as a directed graph with labeled edges. The graph has one vertex for each user/host. For any pair of vertices (u, v) , there is a directed edge from u to v if objects can be copied from u to v . The edge labels can be used to model relevant information about the physical network and may include information such as bandwidth, delay, availability, etc. The vertices are characterized by their object library, object requests made to other vertices, and object requests satisfied.

To operate effectively, the darknet has a small number of technological and infrastructure requirements, which are similar to those of legal content distribution networks: The static hardware requirements to support a darknet are:

1. The *injection* requirement comprises technologies, devices and mechanisms that convert objects into a form, in which they can be transmitted and consumed in a darknet. Examples include audio and video compression algorithms and tools, CD and DVD readers, and programs that circumvent content protection systems (cracks). Injection provides darknets with new objects.
2. Mechanisms for *storage* and *replication* are required to allow users to make and keep copies of objects and to support the store and forward model of peer to peer networks. Examples include tapes, CDs, DVDs, and computer hard disks.
3. *Ubiquitous rendering devices* required to allow consumption of objects. Examples include portable music players, computers and consumer electronics DVD players and television sets.

The following core network related requirements correspond roughly to the components of the graph model outlined above:

1. Any darknet requires nodes that operate as object *sources*. These correspond to users who let at least some other users copy objects available to them.

2. Similarly, any darknet will contain *destination nodes* — users who want copies of objects. Often, nodes operate as both sources and destinations.
3. *Transmission links* are necessary to move copies of objects from source nodes to destination nodes. The Internet is the link that supports today’s peer to peer networks. The postal service and hand carried CDRs (sneakernet) support other darknets.
4. *Search engines* or other introduction mechanisms allow new and existing users to find objects on the darknet.

The dramatic rise in the efficiency of the darknet can be traced back to the general technological improvements in these infrastructure areas. At the same time, most attempts to fight the darknet focus on limiting or auditing one or more of the infrastructure items. Legal action has traditionally targeted search engines and source nodes. As we will describe later in the paper, this has been partially successful. The drive for legislation on mandatory watermarking aims to deprive the darknet of rendering devices. We will argue that watermarking approaches are technically flawed and unlikely to have any material impact on the darknet. Similarly, most content protection systems are meant to prevent or delay the injection of new objects into the darknet. However, no such system constitutes an impenetrable barrier; later, we will discuss the merits of some popular systems.

We see no technical impediments to the darknet becoming increasingly efficient (measured by aggregate library size and available bandwidth). However, the darknet infrastructure is under legal attack. In this paper, we trace the historical and current attacks on darknets and speculate on the technical and legal future of sharing technologies, concentrating particularly, but not exclusively, on peer to peer networks.

The rest of this paper is structured as follows: Section II analyzes different manifestations of the darknet with respect to their robustness to attacks on the infrastructure requirements described above and speculates on the future development of the darknet. Section III describes content protection mechanisms, their probable effect on the darknet, and the impact of the darknet upon them. In Sect. IV and V, we speculate on the situations in which the darknet will be effective, and how businesses may need to behave to compete effectively with it.

II The Evolution of the Darknet

We classify the different manifestations of the darknet that have come into existence in recent years with respect to the five infrastructure requirements described and analyze weaknesses and points of attack.

As a system, the darknet is subject to a variety of attacks. While legal action, aimed at deterring widespread infringement, continues to be the most powerful challenge to the darknet, the darknet is also subject to a variety of other common threats (e.g. viruses, spamming) that, in the past, have lead to minor disruptions of the darknet. They threaten to become considerably more damaging.

In this section we consider the potential impact of legal developments on the darknet. Most of our analysis focuses on system robustness, rather than on detailed legal questions. We regard legal questions only with respect to their possible effect: the failure of certain nodes or links (vertices and edges of the graph defined above). In this sense, we are investigating a well known problem in distributed systems.

II.1 Early Small Worlds Networks

Prior to the 1990s, copying was organized around groups of friends and acquaintances.⁸⁶⁹ The copied objects consisted mainly of music on cassette tapes and computer programs. The rendering devices were widely available tape players and the computers of the time (see fig. 1). Content injection was trivial, since most objects were either not copy protected or, if they were equipped with copy protection mechanisms, the mechanisms were easily defeated. The distribution network was a “sneaker net” of floppy disks and tapes (storage), which were exchanged in person by members of a group or were sent by postal mail. The bandwidth of this network — albeit small by today’s standards — was sufficient for the objects of the time. The main limitation of the sneaker net, with its mechanical transport layer, was latency: It could take days or weeks to obtain a copy of an object. Another serious limitation of these networks was the lack of a sophisticated search engine.

There were some attempts to prosecute individuals who were trying to sell copyrighted objects they had obtained from the darknet (commercial piracy). However, the darknet as a whole was never under significant legal threat. Reasons may have included its limited commercial impact and the protection from legal surveillance afforded by sharing amongst friends.

The sizes of object libraries available on such networks are strongly influenced by the interconnections between the networks. For example, schoolchildren may copy content from their “family network” to their “school network” and thereby increase the size of the darknet object library available to each. Such networks have been studied extensively and are classified as “interconnected small worlds networks”.⁸⁷⁰ There are several popular examples of the characteristics of such systems. For example, most people have a social group of a few score of people. Each of these people has a group of friends that partly overlap with their friends’ friends, and also introduces more people. It is estimated that, on average, each person is connected to every other person in the world by a short chain of people from which arises the term “six degrees of separation.” These findings are remarkably broadly applicable.⁸⁷¹ We suspect that these findings have implica-

⁸⁶⁹ Prior to this, some early computer users had access to ftp servers, usenet, and bulletin boards. These provided high bandwidth access to computer programs, and later to objects, such as images scanned in violation of copyright. However, the size of the communities served by these darknets was negligible.

⁸⁷⁰ See: Watts, Strogatz (1998).

⁸⁷¹ See, e.g.: Milgram (1967); Albert, Jeong, Barabási (1999).

tions for copying on darknets, and we will return to this point when we discuss the darknets of the future later in this paper.

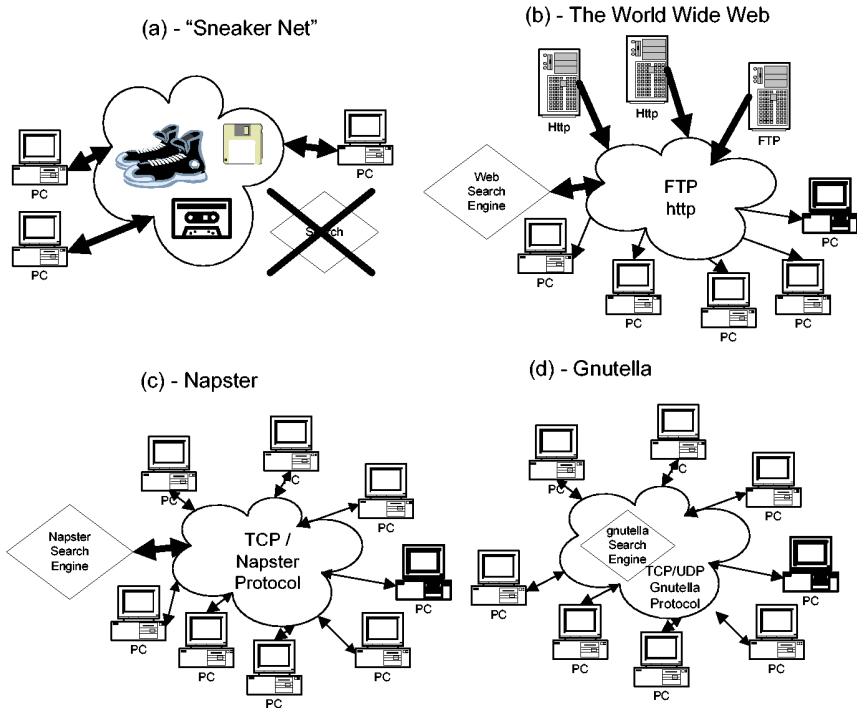


Fig. 1. Historical evolution of the Darknet. We highlight the location of the search engine (if present) and the effective bandwidth (thicker lines represent higher bandwidth). Network latencies are not illustrated, but are much larger for the sneaker net than for the IP-based networks.

The small worlds darknet continues to exist and indeed remains dominant for certain types of content. However, a number of technological advances have given rise to new forms of the darknet that have superseded the small worlds manifestation for some object types (e.g. audio).

II.2 Central Internet Servers

By 1998, a new form of the darknet began to emerge from technological advances in several areas. The internet had become mainstream, and could be used by anyone seeking to connect users with a centralized service or with each other. The continuing fall in the price of mass storage together with advances in compression technology had also crossed the threshold at which storing large numbers of audio files was no longer an obstacle to mainstream users. Additionally, the power of computers had crossed the point at which they could be used as rendering devices for multimedia content. finally, “CD ripping” (from unprotected CDs) became a convenient, broadly available method for content injection.

The first embodiments of this new darknet were central internet servers with large collections of MP3 audio files. A fundamental change that came with these servers was the use of a new distribution network: The internet displaced the sneaker net — at least for audio content. This solved several problems of the old darknet.

Firstly, latency was reduced drastically. Secondly, and more importantly, discovery of objects became much easier because of simple and powerful search mechanisms — most importantly general purpose world wide web search engines. The local view of the small world was replaced by a global view of the entire collection accessible to all users. The main characteristic of this form of the darknet was centralized storage and search — a simple architecture that mirrored mainstream internet servers.

Centralized or quasi-centralized distribution and service networks make sense for legal online commerce. Bandwidth and infrastructure costs tend to be low, and having customers visit a commerce site means the merchant can display adverts, collect profiles, and bill efficiently. Additionally, management, auditing, and accountability are much easier in a centralized model. However, centralized schemes work poorly for illegal object distribution because large, central servers are large single points of failure: If the distributor is breaking the law, it is relatively easy to force him to stop. Early MP3 Web and FTP sites were commonly “hosted” by universities, corporations, and ISPs. Copyright holders or their representatives sent “cease and desist” letters to these website operators and web owners citing copyright infringement and in a few cases followed up with legal action.⁸⁷² The threats of legal action were successful attacks on those centralized networks, and MP3 web and FTP sites disappeared from the mainstream shortly after they appeared.

In the language of the model of Sect. I, the centralized server darknet succumbed to a legal attack on its source nodes, whose small number made the attack tractable.

II.3 Peer to Peer Networks

The realization that centralized networks are not robust against attack has provided part of the impetus for the evolution of peer to peer networking and file sharing technologies. In this section, we examine architectures that have evolved. Early systems were flawed because critical components remained centralized (Napster) or because of inefficiencies and lack of scalability of the protocol (gnutella).⁸⁷³ It should be noted that the problem of object location in a massively distributed, rapidly changing, heterogeneous system was new at the time peer to peer systems emerged. Efficient, highly scalable protocols have been proposed since then.⁸⁷⁴

⁸⁷² See: RIAA.

⁸⁷³ See: Javanović, Annexstein, Berman (2001).

⁸⁷⁴ See: Stoica, Morris, Karger, Kaashoek, Balakrishnan (2001); Dabek, Brunskill, Kaashoek, Karger, Morris, Stoica, Balakrishnan (2001).

Early Internet Protocols

Simple peer to peer-like systems have existed on the internet for a long time. The main example is Usenet, which predates the central server darknets described above. While certain parts of Usenet have been and are still being used to distribute certain types of objects illegally, Usenet never became a mainstream darknet and never faced many of the attacks the more recent darknets are exposed to. We note, however, that the problem of endpoint anonymity arose in connection with Usenet. This resulted in work on anonymizing remailers and legal attacks on them.

Napster

Napster was the service that ignited peer to peer file sharing in 1999.⁸⁷⁵ There is little doubt that a major portion of the massive (for the time) traffic on Napster was of objects being transferred in a peer to peer model in violation of copyright law. Napster succeeded where central servers had failed by relying on the distributed storage of objects not under the control of Napster. This moved the injection, storage and replication, source nodes, network distribution, and consumption of objects to users.

However, Napster retained a quasi-centralized database with an index searchable on the file name. The centralized database itself became a legal target.⁸⁷⁶ Napster was first enjoined to deny certain queries (e.g. “Metallica”) and then to police its network for copyrighted content. As the size of the darknet indexed by Napster shrank, so did the number of users. This illustrates a general characteristic of darknets: there is a correlation between the size and bandwidth of the object library and the appeal of the network for its users. This translates into positive feedback in the number of users: an efficient service quickly gains new users, and vice versa.

Gnutella

The next technology that sparked public interest in peer to peer file sharing was Gnutella. In addition to distributed object storage, Gnutella uses a fully distributed database described more fully in.⁸⁷⁷ Gnutella does not rely upon any centralized server or service — a peer just needs the IP address of one or a few participating peers to (in principle) reach any host on the Gnutella darknet. Second, Gnutella is not really “run” by anyone: it is an open protocol and anyone can write a Gnutella client application. Finally, Gnutella and its descendants have substantial non-infringing uses. This changes its legal standing markedly and places it on a similar legal footing with email. Because email has substantial non-infringing use, it is not under direct legal threat in the jurisdiction of the authors of this paper, even though it may be used to transfer material unlawfully.

⁸⁷⁵ See: napster.

⁸⁷⁶ See: RIAA.

⁸⁷⁷ See: gnutella.

II.4 Robustness of Fully Distributed Darknets

Fully distributed peer to peer systems do not present the single points of failure that led to the demise of central MP3 servers (injection) and Napster (search). It is natural to ask how robust these systems are and what form potential attacks could take. We observe the following weaknesses in Gnutella-like systems:

- Free riding
- Lack of anonymity

Free Riding

Peer to peer systems are often thought of as fully decentralized networks with copies of objects uniformly distributed among the hosts. While this is possible in principle, in practice it is not the case. Recent measurements of libraries shared by gnutella peers indicate that the majority of content is provided by a tiny fraction of the hosts which we term “super peers”.⁸⁷⁸ Although gnutella appears to be a homogeneous peer to peer network of cooperating hosts, in actual fact it has evolved to effectively be another largely centralized system (fig. 2). Free riding (i.e. downloading objects without sharing them) by many gnutella users appears to be main cause of this development. Widespread free riding removes much of the power of network dynamics and may reduce a peer to peer network into a simple unidirectional distribution system from a small number of sources to a large number of destinations. Of course, if this is the case, then the vulnerabilities that we observed in centralized systems (e.g. FTP-servers) are present again. Free riding and the emergence of super-peers have several causes: Peer to peer file sharing assumes that a significant fraction of users adhere to a post-capitalist ideal of sacrificing their own resources for the “common good” of the network. Apparently, most free riders do not seem to adopt this ideology. For example, with 56 kbps modems still being the network connection for most users, allowing uploads constitutes a tangible bandwidth sacrifice. One approach is to make collaboration mandatory. For example, Freenet⁸⁷⁹ clients are required to contribute some disk space. However, enforcing such requirements without a central infrastructure is difficult.

Existing infrastructure is another reason for the existence of super peers. There are vast differences in the resources available to different types of hosts. For example, a T3 connection provides the combined bandwidth of about one thousand 56 kbps telephone connections.

Lack of Anonymity

Users of gnutella who share objects they have stored are not anonymous. Current peer to peer networks permit the server endpoints to be determined, and if a peer-client can determine the IP address and affiliation of a peer, then so can a government agency. Users who share objects illegally face the threat of legal action. This appears to be another motivation for free riding.

⁸⁷⁸ See: Adar, Huberman (2000).

⁸⁷⁹ See: Clarke, Sandberg, Wiley, Hong (2000).

II.5 Attacks⁸⁸⁰

In this section, we analyze the robustness of distributed darknets with global databases. We consider how a variety of counter measures might apply to each of the technological and infrastructure requirements we identified in Sect. 1. These measures can be broadly classified as:

Legal: filing lawsuits against users of the darknet or the operators of its infrastructure. Such attacks remove users from the darknet, but more importantly discourage participation of a much larger group of potential users.

Content protection: A collection of technical measures ranging from hindering injection (DRM) to attempts to make rendering devices reject darknet objects (watermark screening) and forensics (fingerprinting). These techniques are discussed in more detail in Sect. 3.

Network attacks: Like any other network, the darknet is subject to well known attacks, such as denial of service (DoS), spamming and viruses. We do not investigate the legal status of these attacks, but simply note that they are, in principle, possible and, to a very limited degree, appear to have taken place in the past.

Much of the static infrastructure (injection, storage, replication, rendering) has substantial non-infringing uses. Examples of such dual use technologies include audio and video compression tools, CD and DVD players, computers, monitors and television sets. These technologies appear largely immune to legal action. Furthermore, network attacks do not appear to apply in most cases. This leaves content protection as the main class of measures against the static darknet infrastructure. We analyze the effectiveness of these techniques in detail in Sect. III. It appears unlikely that content protection measures alone will have a significant impact on the darknet.

The case of injection is different in the sense that injection tools that circumvent content protection mechanisms are subject to legal action — possibly under the Digital Millennium Copyright Act (DMCA). However, the most relevant recent example of such legal action appears to have been largely unsuccessful. DVD “ripping” tools that circumvent the CSS copy protection system are easily available on the internet.

Attacks against the network infrastructure of the darknet fall mostly into the categories of legal action and network attacks.

Sources

Source nodes of the darknet (i.e. hosts that make objects available to users in violation of copyright law) are subject to legal action. Lack of endpoint anonymity makes these hosts identifiable. Because of the prevalence of super peers the darknet depends on a relatively small set of powerful hosts, and these hosts are promising targets for attackers.

⁸⁸⁰ See: *Hauser, Wenz* within this book on page 206.

Darknet hosts owned by corporations are typically easily removed. Often, these hosts are set up by individual employees without the knowledge of corporate management. Generally corporations respect intellectual property laws. This together with their rational aversion to lawsuits, and their centralized network of hierarchical management, makes it relatively easy to remove darknet hosts in the corporate domain.

While the structures at universities are typically less hierarchical and strict than those of corporations, similar rules often apply.

If the .com and .edu OC-3 and OC-12 lines were pulled from under a darknet, the usefulness of the network would be impaired. Today, this would leave DSL, ISDN, and cable modem users as the high bandwidth servers of objects. We believe limiting source hosts to this class would present a far less effective piracy network today from the perspective of acquisition because of the relative rarity of high bandwidth consumer connections, and hence users would abandon this darknet. However, consumer broadband is becoming more popular, so in the long run it is probable that there will be adequate consumer bandwidth to support an effective consumer darknet.

The obvious next legal escalation is to bring direct or indirect (through the affiliation) challenges against users who illegally share large libraries of material. This is already happening and the legal actions appear to be successful.⁸⁸¹ This requires the cooperation of ISPs in identifying their customers, which appears to be forthcoming due to requirements that the carrier must take to avoid liability and, in some cases, because of corporate ties between ISPs and content providers. Once again, free riding makes this attack strategy far more tractable.

In addition to legal action, sources are subject to different kinds of denial of service attacks. These attacks become also more viable in the presence of widespread free riding.

Destination Nodes

Destination nodes suffer from the same endpoint anonymity problem as source nodes. In principle, similar legal attacks apply. In practice, destination nodes are better protected by their larger numbers.

Transmission

Attacks on transmission typically take the following forms. first, there have been attempts to identify and block darknet traffic on the internet. While such attacks may succeed with today's peer to peer systems, they are easily prevented by encrypting the darknet traffic. A second type of countermeasure is to limit the upload bandwidth of users who are suspected of providing large amounts of data into the darknet. While measures of this type may work against darknets with a relatively small set of super peers, they appear significantly less effective in darknet environments with more broadly distributed source nodes.

⁸⁸¹ See: Clarke.

Search Engine

In Gnutella-style darknets, the search engine is integrated into the nodes. Thus, legal measures against the search engine are largely equivalent to legal measures against source and destination nodes, as described above. However, the global search engine has important implications for the feasibility of legal measures, as it removes endpoint anonymity and makes nodes globally identifiable. That is, the identity (IP address) of any source node is exposed through the global search engine to any client.

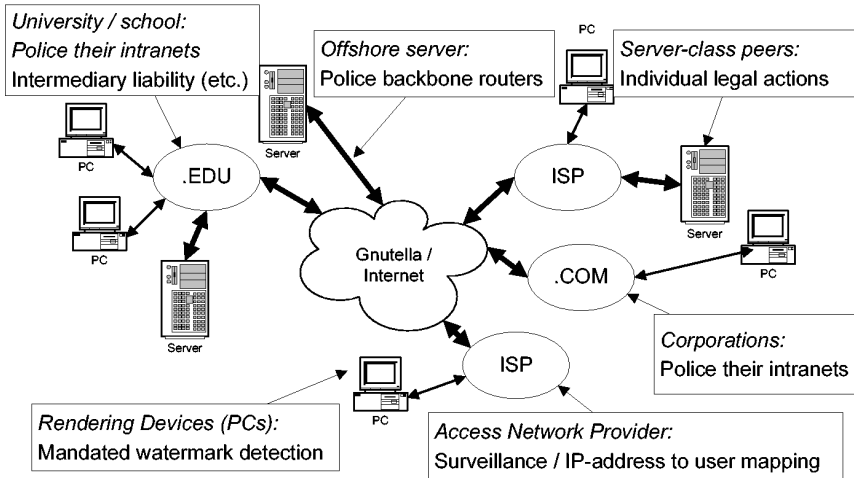


Fig. 2. Policing the darknet. Gnutella-style networks appear hard to police because they are highly distributed, and there are thousands or millions of peers. Looking more closely there are several potential vulnerabilities.

There are some technological workarounds to overcome the vulnerability presented by the lack of endpoint anonymity: anonymizing routers, overseas routers and object fragmentation complicate the effort required by law enforcement to determine the original source of unlawfully transferred bits. For example, Freenet tries to hide the identity of the hosts storing any given object by means of a variety of heuristics, including routing the object through intermediate hosts and providing mechanisms for easy migration of objects to other hosts. Similarly, Mnemosyne⁸⁸² organizes object storage such that individual hosts may not know what objects are stored on them. It is conjectured in Hand, Roscoe⁸⁸² that this may amount to common carrier status for the host. A detailed analysis of the legal or technical robustness of these systems is beyond the scope of this paper. However, all such systems introduce the possibility of intermediary liability for the individuals who provide the “final hop.”

⁸⁸² See: Hand, Roscoe (2000).

Conclusions

The most relevant attacks we have identified exploit the lack of endpoint anonymity and are aided by the effects of free riding. We have seen effective legal measures on all peer to peer technologies that are used to provide global access to copyrighted material. Centralized web servers were effectively closed down. Napster was effectively closed down. Gnutella and KaZaA are under threat because of free rider weaknesses and lack of endpoint anonymity.

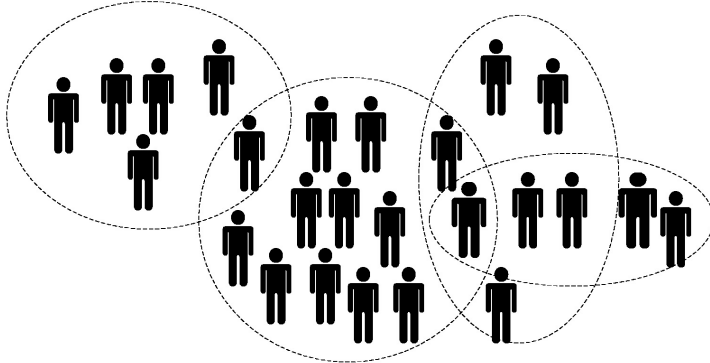


Fig. 3. Interconnected small worlds darknets. Threats of surveillance and prosecution may discourage participation in global darknets. In response, darknets form around social groups for which surveillance of illicit activity is unlikely. These darknets will use high bandwidth, low latency communications (intranets and the internet) and are supported by search engines. Custom applications, Instant Messenger style applications or simple shared file systems host the darknet. People's social groups overlap so objects available in one darknet diffuse to others: in the terminology used in this paper, each peer that is a member of more than one darknet is an introduction host for objects obtained from other darknets.

Should Gnutella-style systems become unviable as darknets, systems such as Freenet or Mnemosyne might replace them. It is hard to predict further escalation, but we note that the DMCA is a far reaching (although not fully tested) example of a law that is potentially quite powerful. We believe it probable that there will be ongoing technical efforts to sidestep existing laws, followed by new laws, or new interpretations of old laws, in the next few years. The rapid build out of consumer broadband, the decreasing price of storage, and the fact that personal computers are effectively establishing themselves as centers of home entertainment are technical developments that will continue to drive darknet demand.

Lack of endpoint anonymity is a direct result of the globally accessible global object database, and it is the existence of the global database that most distinguishes the newer darknets from the earlier small worlds. At this point, it is hard to predict whether the darknet will be able to retain this global database in the long term, but it seems clear that legal setbacks to global index peer to peer will continue.

II.6 Small Worlds Networks Revisited

In this section we try to predict the evolution of the darknet should global peer to peer networks be effectively stopped by legal or other means. The globally accessible global database is the only infrastructure component of the darknet that can be disabled in this way. The other enabling technologies of the darknet (injection, distribution networks, rendering devices, storage) will not only remain available, but will rapidly increase in power. We stress that the networks described in this section (in most cases) provide poorer services than the global network.

In the absence of a global database, small worlds networks could again become the prevalent form of the darknet. However, these small worlds will be more powerful than they were in the past. With the widespread availability of cheap CD and DVD readers and writers as well as large hard disks, the bandwidth of the sneaker net has increased dramatically, the cost of object storage has become negligible and object injection tools have become ubiquitous. Furthermore, the internet is available as a distribution mechanism that is adequate for audio for most users, and is becoming increasingly adequate for video and computer programs. In light of strong cryptography, it is hard to imagine how sharing could be observed and prosecuted as long as users do not share with strangers.

Students in dorms will establish darknets to share content in their social group. These darknets may be based on simple file sharing, DVD-copying, or may use special application programs or servers: for example, a chat or instant messenger client enhanced to share content with members of your buddy list. Each student will be a member of other darknets: for example, their family, various special interest groups, friends from high school, and colleagues in part time jobs (fig. 3). If these small worlds are sufficiently well connected, we can anticipate that content will rapidly diffuse between darknets. Since the legal exposure of such sharing is quite limited, we believe that sharing amongst socially oriented groups will increase.

The limited exposure of sharing with strangers does not imply that such sharing will become universal. Non-technical admonitions will continue to discourage users from sharing. Such counsel may originate from parents, employers, or educators. The associated threats and possibility of discovery will factor into each individuals decision to share.

Small worlds networks suffer from the lack of a global database; each user can only see the objects stored by his small world neighbors. This raises a number of interesting questions about the network structure and object flow:

- What graph structure will the network have? For example, will it be connected? What will be the average distance between two nodes?
- Given a graph structure, how will objects propagate through the graph? In particular, what fraction of objects will be available at a given node? How long does it take for objects to propagate (diffuse) through the network?

Questions of this type have been studied in different contexts in a variety of fields (mathematics, computer science, economics, physics, and biology). A number of empirical studies seek to establish structural properties of different types of small world networks, such as social networks⁸⁸³ and the world wide web.⁸⁸⁴ These works conclude that the diameter of the examined networks is small, and observe further structural properties, such as a power law of the degree distribution.⁸⁸⁵ A number of authors seek to model these networks by means of random graphs, in order to perform more detailed mathematical analysis on the models⁸⁸⁶ and, in particular, study the possibility of efficient search under different random graph distributions⁸⁸⁷. We will present a quantitative study of the structure and dynamics of small worlds networks in an upcoming paper, but to summarize:

- For popular titles, small worlds darknets can be extremely efficient: very few peers are needed to satisfy requests for “top 20” books, songs, movies or computer programs. If darknets are interconnected, we expect the effective injection rate (injection from other networks) rate to be large. If darknet clients are enhanced to seek out new popular content, as opposed to the user demand based schemes of today, small worlds darknets could become very efficient.
- Less popular titles, will be harder or impossible to find, depending on the network parameters.
- Time sensitive objects will not be available.

For popular titles, small world darknets may provide a quality of service that matches that of peer to peer networks with global databases; for less popular titles, they may suffer from a reduced library size and latency.

III Introducing Content into the Darknet

Our analysis and intuition have led us to believe that efficient darknet replication and propagation will remain a fact of life. In this section we examine rights management technologies that are being deployed to limit the introduction rate of content into the darknet.

III.1 Conditional Access Systems

A conditional access system is a simple form of rights management system in which subscribers are given access to objects based (typically) on a service contract. Digital rights management systems often perform the same function, but typically impose restrictions on the use of objects after unlocking.

⁸⁸³ See: Milgram (1967).

⁸⁸⁴ See: Albert, Jeong, Barabási (1999).

⁸⁸⁵ See: Barabási, Albert (1999).

⁸⁸⁶ See: Aiello, Chung, Lu (2001); Cooper, Frieze (2001); Newman (1999); Newman, Watts, Strogatz (2002).

⁸⁸⁷ See: Kleinberg (2000/2001).

Conditional access (CA) systems such as cable, satellite TV, and satellite radio offer little protection against objects being introduced into the darknet from subscribing hosts. A conditional access system customer has no access to channels or titles to which they are not entitled, and has essentially unencumbered use of channels that he has subscribed or paid for. This means that an investment of \$100 (at time of writing) on an analog video capture card is sufficient to obtain and share TV programs and movies. Some CA systems provide post unlock protections but they are generally cheap and easy to circumvent.

Thus, conditional access systems provide a widely deployed, high bandwidth source of video material for the darknet. In practice, the large size and low cost of CA-provided video content will limit the exploitation of the darknet for distributing video in the near term.

The same can not be said of the use of the darknet to distribute conditional access system broadcast keys. At some level, each head end (satellite or cable TV head end) uses an encryption key that must be made available to each customer (it is a broadcast), and in the case of a satellite system this could be millions of homes. CA system providers take measures to limit the usefulness of exploited session keys (for example, they are changed every few seconds), but if darknet latencies are low, or if encrypted broadcast data is cached, then the darknet could threaten CA system revenues.

We observe that the exposure of the conditional access provider to losses due to piracy is proportional to the number of customers that share a session key. So, cable operators are in a safer position than satellite operators because a cable operator can narrowcast more cheaply.

III.2 DRM Systems

A classical DRM system is one in which a client obtains content in protected (typically encrypted) form, with a license that specifies the uses to which the content may be put. Examples of licensing terms that are being explored by the industry are “play on these three hosts,” “play once,” “use computer program for one hour,” etc.

The license and the wrapped content are presented to the DRM system whose responsibility is to ensure that:

- The client cannot remove the encryption from the file and send it to a peer.
- The client cannot “clone” its DRM system to make it run on another host.
- The client obeys the rules set out in the DRM license.
- The client cannot separate the rules from the payload.

Advanced DRM systems may go further. Some such technologies have been commercially very successful — the content scrambling system used in DVDs, and (broadly interpreted), the protection schemes used by conditional access system providers fall into this category, as do newer DRM systems that use the internet as a distribution channel and computers as rendering devices. These technologies are appealing because they promote the establishment of new businesses and reduce distribution costs. If costs and licensing terms are appealing to producers

and consumers, then the vendor thrives. If the licensing terms are unappealing or inconvenient or the costs are too high then the business will fail. The DivX “DVD” rental model failed on most or all of these metrics, but CSS-protected DVDs succeeded beyond the wildest expectations of the industry.

On personal computers, current DRM systems are software only systems using a variety of tricks to make them more or less hard to subvert. DRM enabled consumer electronics devices are also beginning to emerge.

In the absence of the darknet, the goal of such systems is to have comparable security to competing distribution systems — notably the CD and DVD — so that programmable computers can play an increasing role in home entertainment.

DRM systems strive to be BOBE (break once, break everywhere)-resistant. That is, suppliers anticipate that individual instances (clients) of all security systems, whether based on hardware or software, will be subverted. If a client of a system is subverted, then all content protected by that DRM client can be unprotected. If the break can be applied to any other DRM client of that class so that all of those users can break their systems, then the DRM-scheme is BOBE-weak. If, on the other hand, knowledge gained breaking one client cannot be applied elsewhere, then the DRM system is BOBE-strong.

Most commercial DRM systems have BOBE exploits, and we note that the darknet applies to DRM hacks as well. The CSS system is an exemplary BOBE weak system. The knowledge and code that comprised the DeCSS exploit spread uncontrolled around the world on websites, newsgroups, and even T shirts, in spite of the fact that, in principle, the Digital Millennium Copyright Act makes it a crime to develop or distribute these exploits.

A final characteristic of existing DRM systems is renewability. Vendors recognize the possibility of exploits, and build systems that can be field updated.

It is hard to quantify the effectiveness of DRM systems for restricting the introduction of content into the darknet from experience with existing systems. Existing DRM systems typically provide protection for months to years; however, the content available to such systems has to date been of limited interest, and the content that is protected is also available in unprotected form. The one system that was protecting valuable content (DVD video) was broken very soon after compression technology and increased storage capacities and bandwidth enabled the darknet to carry video content.

III.3 Software

The DRM systems described above can be used to provide protection for software, in addition to other objects (e.g. audio and video). Alternatively, copy protection systems for computer programs may embed the copy protection code in the software itself.

The most important copy protection primitive for computer programs is for the software to be bound to a host in such a way that the program will not work on an unlicensed machine. Binding requires a machine ID: this can be a unique

number on a machine (e.g. a network card MAC — media access control — address), or can be provided by an external dongle.

For such schemes to be strong, two things must be true. first, the machine ID must not be “virtualizable.” For instance, if it is trivial to modify a network card driver to return a different MAC address, then the software–host binding is easily broken. Second, the code that performs the binding checks must not be easy to patch. A variety of technologies that revolve around software tamper resistance can help here.⁸⁸⁸

We believe that binding software to a host is a more tractable problem than protecting passive content, as the former only requires tamper resistance, while the latter also requires the ability to hide and manage secrets. However, we observe that all software copy protection systems deployed thus far have been broken. The definitions of BOBE strong and BOBE weak apply similarly to software. Furthermore, once software is broken, the hacks or patched software are just as much subject to the dynamics of the darknet as passive content.

IV Policing Hosts

If there are subverted hosts, then content will leak into the darknet. If darknet propagation is efficient, then content will be available to all interested peers. In this section we evaluate technologies proposed for limiting output, or provide forensic information that allows users who inject objects in violation of copyright or contract to be identified.

IV.1 Watermarking

Watermarking embeds an “indelible” invisible mark in content.⁸⁸⁹ A plethora of schemes exist for audio/video and still image content and computer programs.

There are a variety of schemes for exploiting watermarks for content protection. These schemes are implemented in output devices. Consider a rendering device that locates and interprets watermarks. If a watermark is found then special action is taken. For example, the output device may:

Restrict behavior: For example, a bus adapter may refuse to pass content that has the “copy once” and “already copied once” bits set.

Require a license to play: For example, if a watermark is found indicating that content is rights–restricted then the renderer may demand a license indicating that the user is authorized to play the content.

Such systems were proposed for audio content — for example the secure digital music initiative (SDMI),⁸⁹⁰ and are under consideration for video by the copy protection technical working group (CPTWG).⁸⁹¹

⁸⁸⁸ See: Aucsmith (1996).

⁸⁸⁹ See: *Petitcolas* within this book on page 81.

⁸⁹⁰ See: SDMI.

⁸⁹¹ See: CPTWG.

There are several reasons why it appears unlikely that such systems will ever become an effective anti-piracy technology. From a commercial point of view, building a watermark detector into a device renders it strictly less useful for consumers than a competing product that does not have one, and such detectors impose a “tax” in performance and cost on consumers who are using devices for perfectly lawful activities. Hence watermarking schemes are unlikely to be widely deployed, unless mandated by legislation. The recently proposed Hollings bill is a step along these lines.⁸⁹² Even with legislation, they are likely to meet severe resistance.

We contrast watermark based policing with classical DRM: If a general purpose device is equipped with a classical DRM system, it can play all content acquired from the darknet, and have access to new content acquired through the DRM channel. This is in stark distinction to reduction of functionality inherent in watermark based policing.

Even if watermarking systems were mandated, this approach is likely to fail due to a variety of technical inadequacies. The first inadequacy concerns the robustness of the embedding layer. We are not aware of systems for which simple data transformations cannot strip the mark or make it unreadable.⁸⁹³ Marks can be made more robust, but in order to recover marks after adversarial manipulation, the reader must typically search a large phase space, and this quickly becomes untenable. In spite of the proliferation of proposed watermarking schemes, it remains doubtful whether robust embedding layers for the relevant content types can be found.

A second inadequacy lies in unrealistic assumptions about key management. Most watermarking schemes require widely deployed cryptographic keys. Standard watermarking schemes are based on the normal cryptographic principles of a public algorithm and secret keys. Most schemes use a shared key between marker and detector. In practice, this means that all detectors need a private key, and, typically, share a single private key. It would be naïve to assume that these keys will remain secret for long in an adversarial environment. Once the key or keys are compromised, the darknet will propagate them efficiently, and the scheme collapses. There have been proposals for public key watermarking systems. However, so far, this work does not seem practical and the corresponding schemes do not even begin to approach the robustness of the cryptographic systems whose name they borrow.

A final consideration relates to the location of mandatory watermark detectors in client devices. On open computing devices (e.g. personal computers), these detectors could, in principle, be placed in software or in hardware. Placing detectors in software would be largely meaningless, as circumvention of the detector would be as simple as replacing it by a different piece of software. This includes detectors placed in the operating system, all of whose components can be easily replaced, modified and propagated over the darknet.

⁸⁹² See: Hollings.

⁸⁹³ See: Kirovski, Petitcolas (2003); *Petitcolas* within this book on page 81.

Alternatively, the detectors could be placed in hardware (e.g. audio and video cards). In the presence of the problems described this would lead to untenable renewability problems — the hardware would be ineffective within days of deployment. Consumers, on the other hand, expect the hardware to remain in use for many years. finally, consumers themselves are likely to rebel against “footing the bill” for these ineffective content protection systems. It is virtually certain that the darknet would be filled with a continuous supply of watermark removal tools based on compromised keys and weaknesses in the embedding layer. Attempts to force the public to “update” their hardware would not only be intrusive, but impractical.

In summary, attempts to mandate content protection systems based on watermark detection at the consumer’s machine suffer from commercial drawbacks and severe technical deficiencies. These schemes, which aim to provide content protection beyond DRM by attacking the darknet, are rendered entirely ineffective by the presence of even a moderately functional darknet.

IV.2 Fingerprinting

Fingerprint schemes are based on similar technologies and concepts to watermarking schemes.⁸⁹⁴ However, whereas watermarking is designed to perform a-priori policing, fingerprinting is designed to provide a-posteriori forensics.

In the simplest case, fingerprinting is used for individual sale content (as opposed to super-distribution or broadcast — although it can be applied there with some additional assumptions). When a client purchases an object, the supplier marks it with an individualized mark that identifies the purchaser. If the marked content appears on a darknet, a policeman can identify the source of the object and the offender can be prosecuted or other action can be taken.

Fingerprinting suffers from fewer technical problems than watermarking. The main advantage is that no widespread key distribution is needed — a publisher can use whatever secret or proprietary fingerprinting technology they choose, and is entirely responsible for the management of their own keys.

Fingerprinting has one problem that is not found in watermarking. Since each fingerprinted copy of a piece of media is different, if a user can obtain several different copies, he can launch collusion attacks (e.g. averaging). In general, such attacks are very damaging to the fingerprint payload.

It remains to be seen whether fingerprinting will act as a deterrent to theft. There is currently no legal precedent for media fingerprints being evidence of crime, and this case will probably be hard to make since detection is a statistical process with false positives, and opportunity for deniability. However, we anticipate that there will be uneasiness in sharing a piece of content that may contain a person’s identity and that ultimately leaves that person’s control.

Note also that, with widely distributed watermarking detectors, it is easy to see whether a watermark has been successfully removed. There is no such assurance

⁸⁹⁴ See: *Herre* within this book on page 93.

for determining whether a fingerprint has been successfully removed from an object because users are not necessarily knowledgeable about the fingerprint scheme or schemes in use. However, if it turns out that the deterrence of fingerprinting is small (i.e. everyone shares their media regardless of the presence of marks), there is probably no reasonable legal response. Finally, distribution schemes in which objects must be individualized will be expensive.

V Conclusions

There are no inherent technical impediments to darknet based object sharing technologies growing in usability, library size, aggregate bandwidth and efficiency, but the legal future of darknet technologies is less certain. We have described successful or partially successful legal attacks on all network based object sharing technologies in widespread use today. We anticipate further escalation of attacks and of darknet technologies to remove the vulnerabilities that were exploited in previous attacks. We have analyzed the infrastructure components necessary to support arbitrary darknets, and have argued that, while some of the infrastructure components appear immune to legal or technological attack, some vulnerabilities will remain.

The largest vulnerability arises from the exposure of a user's identity, either directly or indirectly, to law enforcement masquerading as a peer. This vulnerability arises if users share with unknown or anonymous peers, and is a consequence of registering hosts and objects with a global database or other database without user access control. Should the threat of legal action make sharing among anonymous users too risky for average users, then we have argued that darknets will form around smaller, access controlled small worlds groups for which the risk of surveillance is smaller.

The reduced exposure afforded by small worlds darknets to their users may come at the price of diminished quality of service. The library size, availability, and latency of a small world darknet will always be inferior to that of a global darknet. This will almost certainly mean that small worlds darknets will be impractical for sharing less popular objects and time sensitive objects. On the other hand, even moderately efficient small worlds darknets are likely to provide high quality of service for the most popular objects.

It is our conjecture that darknets will survive, but the efficiency and size of these future darknets is uncertain. In the remainder of this section we speculate on the technical and business implications of the continued existence of darknets of varying levels of efficiency on the commerce of digital goods.

V.1 Technological Implications

Darknets replicate objects. An efficient darknet replicates objects rapidly, and makes the original and its replicas available to an expanding group of users. If the darknet is an efficient global darknet then all users can access an object immediately after it is introduced. If architectural deficiencies or attacks reduce

the efficiency of a global darknet then significant time and effort may be required to obtain a copy of an object. If no global darknet exists, but a user is a member of one or more small worlds darknets then users must wait until an object reaches their small world — either by diffusing from an interconnected small world, or through direct injection.

Classical DRM systems inhibit the injection of objects into darknets. However, we must always assume that a fraction of DRM systems are subverted, or objects are introduced into the darknet through other channels. In light of the arguments in the previous paragraph we conclude that DRM systems will be effective in limiting the widespread availability of objects for isolated small worlds darknets, but will be ineffective security measures in the presence of efficient global darknets.

The interesting cases arise between these two extremes — in the presence of a darknet which is connected but in which factors such as latency, limited bandwidth or the absence of a global database limit the speed with which objects propagate. It appears that quantitative studies of the effective “diffusion constant” of different kinds of darknets and objects would be highly useful in elucidating the dynamics of DRM systems and the darknet.

Proposals for systems involving mandatory watermark detection in rendering devices try to impact the effectiveness of the darknet directly by trying to detect and eliminate objects that originated in the darknet appear flawed. In addition to severe commercial and social problems, these schemes suffer from serious technical deficiencies, which argue against their future value. We conclude that such schemes are doomed to failure.

V.2 Business in the Face of the Darknet

Darknets are a competitor to legal commerce, and the normal rules of competition apply. The level of competition of a darknet for an industry depends on its efficiency and effective price compared to the convenience and price of the competing legal channels (as well as other social factors like the price sensitivity and honesty of the users).

Historically, the efficiency of a darknet has been affected by the legal and technical attacks upon it. We have argued that global darknets have inherent vulnerabilities that can be exploited to reduce library size and aggregate bandwidth. Clearly, the level of competition provided by a darknet depends on the attacks it is exposed to, and we assume that businesses will continue to invest in such attacks. We have argued that these attacks may reduce the quality of service of darknets, even if they may not completely eliminate them.

A moderately efficient darknet will provide pressure on the price and convenience of legal channels for businesses. There are many technical and social factors that determine the competitiveness of a darknet, and we will list those that seem particularly important. first, the size of the shared objects: Current peer to peer darknets appear adequate for audio, but are not adequate for video for most users. Second, the behavior of the customers: corporate customers are unlikely

to engage in widespread sharing of digital objects in violation of contract or copyright. However, it appears that many people share audio files without compunction. Third, the distribution size: mass market media is widely distributed and widely interesting. This implies many potential injection hosts, and high demand driving darknet replication. In contrast, personalized documents or premium business reports are far less likely to be introduced and replicated. Fourth, the convenience of the legal channel: convenience can take many forms: a DRM-protected object may be less convenient than an unprotected object; a native digital representation of an object from a darknet may be more appealing to some users than an object embedded in a physical artifact (e.g. a CD). fifth, time: if darknets are only moderately efficient then there will be a delay before a new object is widely available. Of course the price of the object is a huge factor, and there are many others.

We do not believe that darknets will drive the cost of all digital goods to zero, but it appears likely that the effects on some types of mass market digital commerce will be significant.

Acknowledgements: We are grateful to Cormac Herley, Rico Malvar, John Manferdelli and Yacov Yacobi, for many useful comments, ideas, and discussions.

4 Digital Rights Management: Legal and Political Aspects

4.1 Protection of Digital Content and DRM Technologies in the USA

4.1.1 Protection under US Copyright Law

*Mathias Lejeune*⁸⁹⁵

I Introduction

The modern technologies of the digital age make it very easy to copy and to distribute copies of nearly any kind of content by a mere “maus-click”. Therefore effective Copy Control Systems, nowadays as “Digital Rights Management Systems” or “Copy Protection Systems” circumscribed, are the basic condition for the survival of the content industries.

Movie and music industries depend on the U.S. market, which is by far the most important market in the world in terms of economic figures for such kind of products. The most important movie studios f.i. Disney and music publishers f.i. RCA are companies having its headquarters in the USA. Therefore it had to be the United States of America by enacting the “Digital Millennium Copyright Act” (DMCA)⁸⁹⁶ to be the first country to enact laws and regulations specifically tailored to introduce, establish and protect Digital Rights Management Systems.

However not only the content industry, but also the IT-industry, led by the big players like Microsoft and others have become aware of the problems related to illegal copying especially of software products (“software piracy”). Therefore a discussion in the US legal community has started, whether it is appropriate to require hardware manufacturers like IBM, Dell, HP and even certain component manufacturers like Intel to build computer systems with Copy Protection Systems incorporated into the hardware and by doing so, to prevent illegal copying and distribution already at “the source”. The discussion in the USA has been the basis for an initiative to enact respective provisions into the US law led by Senator Hollings, which is therefore known as the “Hollings Bill”⁸⁹⁷.

⁸⁹⁵ Attorney at law, Munich.

⁸⁹⁶ See: Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28 1998); the origin of the DMCA goes back to the “Working Group on Intellectual Property Rights”, which has been established by President Clinton in 1993. Chairman of the working group was Bruce Lehman. The final report of the working group “Intellectual Property and the National Infrastructure” dated September 1995 first made the proposal to add sections to the Copyright Act, in which the subject matter of the DMCA should be addressed.

⁸⁹⁷ See: “Security Systems Standards and Certification Act”, so-called “Hollings Bill”, draft August 6th 2001.

It is the purpose of this article to describe and explain the developments in the USA concerning the legal protection of Digital Rights Management and Copy Protection Systems in recent years.

First I will take a short look on the legal protection of Copy Protection Systems under US law already existing before the DMCA has been enacted (II.). Then I will analyse and explain the provisions of the DMCA. In this context it will be necessary to discuss, whether the DMCA corresponds to certain requirements of general copyright law as well as of the constitution of the United States of America according to the first court decisions concerning the DMCA (III.). Thereafter I will analyse the proposal for hardware implemented copy protection systems, the so called "Hollings Bill" (IV.). Finally I will try to evaluate the US legal situation in general and in its consequences for the legal situation in other countries, especially in regards to the EU directive on harmonization of certain aspects of copyright⁸⁹⁸ (V.). Further the consequences of Digital Rights Management Systems for the average user of computer systems will have to be addressed.

II Legal Protection of Copy Protection Systems before the DMCA Has Been Enacted

The Audio Home Recording Act (AHRA)⁸⁹⁹ of 1992 requires "digital audio recording devices or digital audio interface devices", which are devices able to record audio pieces, to conform to the Serial Copy Management System (SCMS) or any equivalent system approved by the Secretary of Commerce, if imported, manufactured or distributed in the USA. The AHRA covers only digital music recordings. A SCMS shall prevent copies from digital media to digital media, however it can not prevent copies from analog to digital media. Therefore although such devices incorporate SCMS, the manufacturers and distributors of such devices have to pay levies for each device imported, manufactured or distributed.⁹⁰⁰ Computer Systems, although being able to provide copies covered under the AHRA are not included under the AHRA. The import, manufacture or distribution of any device with the primary purpose of any circumvention or deactivation of a Serial Copy Management System is expressly not permitted.⁹⁰¹ Although not directly dealing with copy protection systems two court decisions have to be mentioned in this context, both of them having been issued before the AHRA had been enacted.

⁸⁹⁸ See: Directive 2001/29/EC. Abl. L. 167/10.

⁸⁹⁹ See: Pub. L. No. 102-563, 106 Stat. 4237; technically the AHRA adds sections 1001-1010 to the Copyright Act.

⁹⁰⁰ Insofar the AHRA is quite similar to the German system of levies being imposed on analog and digital devices as compensation for certain rights of users to copy material subject to copyright protection.

⁹⁰¹ The AHRA has been the subject of the decision of the Court of Appeals of the Ninth Circuit in *Recording Industry Association of America v. Diamond Multimedia Systems Inc.* concerning portable MP 3 music players, No. 98-56727, 1999 WL 387265 (9th Circuit, June 15th, 1999).

In 1984 the Supreme Court had to decide whether the manufacture and sale of analog videorecorder systems had to be considered as contributory infringement under the Copyright Act. Two leading Hollywood Studios, Universal City Studios and Walt Disney Productions had sued Sony Corporation of America, manufacturer of the “Betamax” videorecorders.⁹⁰² Plaintiffs sued for damages, such damages being the result of copyright infringement committed by the consumers, who were using these videorecorders for copying of copyrighted material such as movies. The Supreme Court finally rejected the suit. The Supreme Court was of the opinion, that analog videorecorders would not exclusively be used for illegal copying but provided the opportunity of legitimate unobjectionable purposes such as “time-shifting”. Under such circumstances no contributory infringement could be determined.

Based on the Sony decision, the U.S. Court of Appeals for the Fifth Circuit ruled in *Vault v. Quaid* in 1988.⁹⁰³ The defendant was marketing a software program called Ramkey. Ramkey was able to circumvent the copy protection software Prolok, which plaintiff owned and marketed. The 5th Circuit used the same argument the Supreme Court has used in the Sony decision and rejected the suit, because the Ramkey program was able to perform legitimate purposes like the creation of a back up copy of a software program.

Summarizing it is fair to say, that already before the enactment of the DMCA, the legal regime of the USA had to deal with copy protection systems and related problems.

III The Digital Millennium Copyright Act (DMCA) in Detail

III.1 Overview

The Digital Millennium Copyright Act was signed into law by President Clinton on October 28th 1998. The DMCA implements two 1996 World Intellectual Property Organisation (WIPO) treaties, the WIPO Copyright Treaty and the WIPO Performance and Phonograms Treaty. The DMCA is divided into five titles.⁹⁰⁴ However for the purpose of this article, only title I is important. This title implements the WIPO treaties. First it makes certain technical amendments to U.S. law, in order to provide appropriate references and links to the treaties. Second and that is far more important in this context, it creates two new prohibitions to title 17 of the U.S. code: one on the circumvention of technological measures used by copyright owners to protect their work (section 1201) and one

⁹⁰² See: 464 U.S. 417.

⁹⁰³ See: 847 F. 2d 255 (5th Cir. 1988).

⁹⁰⁴ Title I the WIPO Copyright and Performances and Phonograms Treaties Implementation Act of 1998; Title II, the Online Copyright Infringement Liability Limitation Act; Title III, the Computer Maintenance Competition Assurance; Title IV, contains six miscellaneous provisions concerning certain aspects of Copyright Law, f.i. functions of the Copyright Office; Title V, the Vessel Hull Design Protection Act.

on tampering with copyright management information (CMI) (section 1202). Finally title I adds civil and criminal penalties for violating these prohibitions (sections 1203 and 1204).

The basis for the two new prohibitions in the WIPO Copyright Treaty is Art. 11, which states in relevant parts: “*Contracting parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures, that are used by authors in connection with the exercise of their rights under this treaty or the Berne Convention and that restricts acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.*”

With respect to the Integrity of Copyright Management Information Art. 12 of the WIPO Copyright Treaty states in relevant parts: “*Contracting Parties shall provide adequate and effective legal remedies against any person knowingly performing any of the following acts, knowing or with respect to civil remedies having reasonable grounds to know, that it will induce, enable, facilitate or conceal an infringement of any right covered by this Treaty or the Berne Convention. (i) to remove or alter any electronic rights management information without authority; (ii) to distribute, import for distribution, broadcast or communicate to the public, without authority, works or copies of works knowing that electronic rights management information has been removed or altered without authority.*”

To comply with the WIPO treaty, the DMCA adds a new chapter 12 to Title 17 of the U.S. code.

III.2 Section 1201, Circumvention of Copyright Protection Systems

Section 1201 divides technological measures into two categories: measures that prevent unauthorized access to a copyrighted work and measures that prevent unauthorized copying of a copyrighted work. Making or selling devices or services that are used to circumvent either category of technological measure is prohibited in certain circumstances described below according to Section 1201 (a) (2) and (3). As to the act of circumvention in itself, the provision prohibits circumvention of technological measures restricting access to a work, but not the second, restricting of unauthorised copying, Section 1201 (a) (1) (A).⁹⁰⁵

This distinction has been made to allow the public to have the ability to make fair use⁹⁰⁶ of copyrighted works. Since copying of a work may be a fair use under appropriate circumstances, section 1201 does not prohibit the act of circumventing a technological measure, that prevents copying. On the other hand, as the fair use doctrine is not a defence to the act of gaining unauthorized access to a

⁹⁰⁵ See: Section 1201 (a) (1) (A) states: “*No person shall circumvent a technological measure, that effectively controls access to a work protected [...]*”.

⁹⁰⁶ Under U.S. copyright law certain uses of a copyrighted work do not require consent of the owner of the copyright, are therefore not considered to be an infringement of the owners rights, but are expressly allowed under section 107. This principle is called “fair use”.

work, the act of circumventing a technological measure in order to gain access is prohibited.

The following devices or services, which either are produced or designed for the purpose of circumventing a technical measure that effectively controls access of a work (Section 1201 (a) (2)) or effectively protect a right of a copyright owner in a work or portion thereof (Section 1201 (a) (3)) are covered by section 1201, if they fall within any one of the following three categories:

- They are primarily designed or produced to circumvent
- They have only limited commercially significant purpose or use other than to circumvent, or
- They are marketed for use in circumventing with the person's knowledge for use in circumventing

Section 1201 (c) (3) contains language, clarifying that manufacturers of consumer electronics, telecommunications or computing equipment are not required to design their products affirmatively to respond to any particular technological measure.⁹⁰⁷ This so called "no mandate" rule does however apply to all analog videorecorder systems, which have to apply the Macrovision copy protection technology.⁹⁰⁸

Section 1201 provides for two general saving clauses. Section 1201 (c) (1) states, that nothing in section 1201 affects rights, remedies, limitations or defences to copyright infringement, including fair use. Second, section 1201 (c) (2) states that nothing in section 1201 enlarges or diminishes vicarious or contributory copyright infringement.

There are several exceptions to the prohibition of circumvention. The most important exceptions are:

Reverse Engineering, Section 1201 (f)

This exception permits circumvention according to Section 1201 (a) (1) (A) by a person, who has lawfully obtained a right to use a copy of a computer program for the sole purpose of identifying and analysing elements of the program necessary to achieve interoperability with other programs, to the extent, that such acts are permitted under copyright law.

Encryption Research, Section 1201 (g)

Notwithstanding Section 1201 (a) (1) (A) this exception permits circumvention of access control measures and the development of the technological means to do so, in order to identify laws and vulnerabilities of encryption technologies. For the same purposes and notwithstanding Section 1201 (a) (2) and (3) a person may develop or employ technological means to circumvent protection afforded by a technological measure. For the same purposes activities which would otherwise contradict to Section 1201 (a) (2) are permitted under certain circumstances.

⁹⁰⁷ This is basically, what the so-called Hollings Bill would try to achieve, see below under IV.

⁹⁰⁸ See: section 1201 (k).

Personal Privacy, Section 1201 (i)

Notwithstanding Section 1201 (a) (1) (A) this exception permits circumvention, when the technological measure or the work it protects, is capable of collecting or disseminating personally identifying information about the online activities of a natural person.

Security Testing, Section 1201 (j)

Notwithstanding Section 1201 (a) (1) (A) this exception permits circumvention of access control measures and the development of technological means for such circumvention, for the purpose of testing the security of a computer, computer system or computer network, with the authorization of its owner or operator. For the same purposes activities which would otherwise contradict to Section 1201 (a) (2) are permitted under certain circumstances.

III.3 Section 1202, Protection of the Integrity of Copyright Management Information (CMI)

CMI is defined as identifying information about the work, the author, the copyright owner, and in certain cases, the performer, writer or director of the work, as well as the terms and conditions for use of the work, and such other information as the Register of Copyrights may prescribe by regulation. Information concerning users of works is explicitly excluded (subsection c).

This section separates a) dealing with false CMI and b) removal or alteration of CMI. Subsection (a) prohibits the knowing provision or distribution of false CMI, if done with the intent to induce, enable, facilitate, or conceal infringement. Subsection (b) bars the intentional removal or alteration of CMI without authority, as well as the dissemination of CMI or copies of works, knowing that the CMI has been removed or altered without authority. Any liability under subsection (b) requires that the act be done with knowledge of or with respect to civil remedies, with reasonable grounds to know, that it will induce, enable facilitate or conceal an infringement.

III.4 Civil Remedies and Criminal Penalties, Sections 1203 and 1204

Section 1203 gives the courts power to grant a range of equitable as well as monetary remedies similar to those available under the Copyright Act, including statutory remedies. In case of innocent violations the court has a wide range of discretion to reduce or remit damages (section 1203 (c) (5) (A)).

In addition, it is a criminal offence to violate sections 1201 or 1202 wilfully and for purposes of commercial advantage or private financial gain. Under section 1204 penalties range up to a 500.000 USD fine or up to five years imprisonment for a first offence and up to 1.000.000 USD fine or up to 10 years imprisonment for subsequent offences.

III.5 Concerns against the DMCA

By giving right owners more control over the use of copyrighted materials and by providing for exceptions in limited circumstances, the DMCA is a highly complex Act. Based on these circumstances the DMCA has been the subject of critics in the academic world in the US and it had to prove its enforceability in some court rulings.

“Fair Use” Doctrine Imperilled by the DMCA

Although the DMCA in Section 1201 (c) expressly leaves the doctrine of fair use according to Section 107 Copyright Act unaffected, it has been argued, that the DMCA eliminates the doctrine of “fair use”.⁹⁰⁹ There are several arguments mentioned to support this opinion.

The first argument relates to Section 1201 (b). As explained above, this Section bans all devices, which enable circumvention of use restrictions, not only those restrictions that prohibit infringement. Therefore the language of this Section would also include devices designed to bypass use restrictions in order to enable “fair use”. This argument has been discussed by the court in the recent decision of *United States of America v. Elcom Ltd et al.*⁹¹⁰ The court, while understanding the argument, came to the conclusion, that Congress deliberately had enacted the statute in a way that bans all tools for circumvention in order to efficiently fight against unlawful piracy. Therefore according to the court, the result, that it is lawful to circumvent for the purpose of engaging in fair use, while it is unlawful to traffic in tools that allow fair use circumvention is exactly, what Congress intended.⁹¹¹

The court further discussed the argument, that practical difficulties in engaging fair use of digitally protected works eliminate fair use. The court decided, that fair use has not been prohibited by the DMCA, because lawful possessors of copyrighted works may continue to engage in each and every fair use as authorised by law. The court admits, that it may become more difficult to engage in fair use to occur with regard to technologically protected digital works, f.i. quoting may have to occur the old fashioned way by hand or re-typing, rather than by cutting and pasting. However that would not eliminate fair use, because no authority would guarantee a fair user a right to the most technologically convenient way to engage in fair use.⁹¹²

The ruling of the court in *United States of America v. Elcom Ltd et al.* mirrors an earlier decision by the United States District Court, Southern District of New York in the case of *Universal City Studios Inc. et al. v. Shawn C. Reimerdes*

⁹⁰⁹ See: Samuelson (1999): 539; Katz (2001): 66; Nimmer (2000): 727.

⁹¹⁰ In essential parts published in CRI 2002: p. 147ff.

⁹¹¹ See: Fn. 910: p. 148.

⁹¹² See Fn. 910: p. 149; the same arguments are used by the Second Circuit in *Universal City Studios, Inc. v. Eric Corley et al.*, decision dated November 28th 2001, in essential parts published in CRI 2002, 50ff, p. 55.

*et al.*⁹¹³ The court in New York upheld the DMCA against concerns regarding the fair use doctrine with very similar arguments and expressly stated, that the *Sony*⁹¹⁴ decision standards, which might have been a basis to uphold the DeCSS software, which was the subject of that law suit against the DMCA, has been overruled by the DMCA and is no longer applicable in case of any inconsistency with the DMCA.⁹¹⁵

Violation of the First Amendment by the DMCA

One of the most important points in the critics against the DMCA, is the argument, that the DMCA would violate the provisions of the First Amendment of the US constitution.⁹¹⁶ The First Amendment provides for the freedom of speech. As computer code is a means of expressing ideas, the First Amendment must be considered before dissemination of computer code may be prohibited or regulated; in this sense computer code is covered by the First Amendment.⁹¹⁷ Restrictions on expression generally fall into two categories. Restrictions, which apply to the voicing of particular ideas are considered “content-based”. Restrictions, which have nothing to do with the content of the expression and which have only incidental effect of limiting expression are considered “content-neutral”. Whereas content-based restrictions on speech are only permissionable, if they serve compelling state interests by the least restrictive means available, content-neutral restrictions are measured against a less exacting standard. Because restrictions of this type are not motivated by a desire to limit the message, they will be upheld, if they serve a governmental interest and restrict First Amendment freedoms no more necessary.⁹¹⁸

Based on these general principles both the “Reimerdes” court as well as the court in *United States of America v. Elcom Ltd. Et al.* reached the conclusion, that the DMCA does not violate principles of the First Amendment. The “anti trafficking” provisions of Sections 1201 (a) (2) and (3) of the DMCA (so called because the wording reads “[...] or otherwise traffic in any technology [...]”) were considered “content neutral”, because Congress did not target to suppress particular ideas of computer programmers by enacting the DMCA and any impact on the dissemination of programmers were considered purely incidental to the overriding concerns of promoting the distribution of copyrighted works in digital form, while at the same time protecting these works from piracy and other violations of the exclusive rights of copyright holders. The protection of copyrighted works stored on digital media from the vastly expanded risk of piracy in

⁹¹³ See: 111 F. Supp. 2nd 294 (S.D.N.Y. 2000).

⁹¹⁴ See Fn. 902.

⁹¹⁵ See Fn. 913.

⁹¹⁶ “Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press [...]”.

⁹¹⁷ See: *Junger v. Daley*, 209 F. 3rd 481, P. 485 (6th Cir. 2000); detailed discussion in Lee Tien, Publishing Software as a Speech Act, 14 Berkeley Tech. L. J. 629; *Universal City Studios, Inc. v. Eric Corley et al.* Fn. 912: p. 51.

⁹¹⁸ See Fn. 910: p. 148.

the electronic age were considered as important governmental interests. Based on the fact, that pirates are world wide and society increasingly would depend on technological means of controlling access to digital files and systems, the DMCA would not burden “substantially more speech than is necessary to achieve the Government’s asserted goals of promoting electronic commerce, protecting copyrights and preventing electronic piracy”.⁹¹⁹

Congressional Authority to Enact the DMCA

It has further been argued, that Congress exceeded its authority in enacting the DMCA and that therefore the DMCA is unconstitutional. In this context the courts had to examine, whether the Intellectual Property Clause⁹²⁰ and the Commerce Clause⁹²¹ of the constitution grant respective power to Congress.

The District Court for the Northern District of California in *United States of America v. Elcom Ltd. Et al.* first discussed the Commerce Clause. The court noted, that the DMCA prohibits conduct that has a substantial effect on commerce between the states and commerce with foreign nations. Therefore trafficking in or the marketing of circumvention devices would result in a direct effect on interstate commerce. Accordingly the court concluded, that Congress had authority to enact the DMCA under the Commerce Clause.⁹²²

The court then turned to the more difficult question, whether Congress was precluded from enacting the DMCA by restraints by the Intellectual Property Clause. Relying on a decision by the Eleventh Circuit in a similar case⁹²³ the court stated, that a statute is not an unconstitutional exercise of congressional powers, if the statute is not fundamentally inconsistent with the Intellectual Property Clause and is otherwise within the power of Congress to enact under the Commercial Clause.

Based on these guidelines the court reached the conclusion, that the DMCA and its legislative history would clearly demonstrate, that Congress’ intent was to protect intellectual property rights and thus to promote the same purposes served by the Intellectual Property Clause. Therefore the court held the DMCA’s anti device provisions not to be fundamentally inconsistent with the Intellectual Property Clause.

⁹¹⁹ See Fn. 910: p. 149, the same result was reached by the Second Circuit in *Universal City Studios, Inc. v. Eric Corley et al.* Fn. 912: p. 53.

⁹²⁰ “*The Congress shall have power [...] to promote the progress of science and useful arts by securing for limited times to authors and inventors the exclusive rights to their respective writings and discoveries*”, US constitution Art. 1, § 8 cl.8.

⁹²¹ “*The Congress shall have power [...] to regulate commerce with foreign nations and among the several states and with the Indian tribes [...]*” US constitution Art. 1, § 8 cl.3.

⁹²² See: Fn. 910: p.150, opposing Law Professors “*Amici Curiae Brief*” concerning the *Universal City Studios, Inc. v. Eric Corley et al.*, (see: Fn. 912) case, dated 26.1.2001, available under wysiwyg:

//1//http://www.eff.org/IP/Vide...cases/20010126_ny_lawprofs_amicus.html.

⁹²³ See: *United States of America v. Moghadam*, 175 F. 3d 1269 (11th Cir. 1999).

Summarising, it is fair to say, that the courts notwithstanding criticism from the legal community in the USA, which will be addressed further below, regard the DMCA as an enforceable act, that corresponds to the requirements of the Copyright Act as well as to the requirements of the US constitution.

IV The Security Systems Standards and Certification Act (so-called “Hollings Bill”)⁹²⁴

In September 2001 Senator Fritz Hollings introduced a draft for a bill, which has gained considerable public attendance.

Section 101 (a) “*Prohibition of certain devices*” of Title 1 “*Security System Standards*” of the “*Security Systems Standards and Certification Act*” declares it to be unlawful, “*to manufacture, import offer to the public, provide or otherwise traffic in any interactive digital device that does not include and utilise certified security technologies that adhere to the security system standards adopted under section 104*”.

Section 101 (b) provides an exception to Section 101 (a) for “*any previously-owned interactive digital device*”, if such device has legally been manufactured, imported and sold prior to the effective date of regulations adopted under section 104 and if it has not been modified in a way that security technologies have subsequently been removed or altered.

Section 103 (a) makes it unlawful (1) to remove or alter any certified security technology in an interactive digital device or (2) to transmit or make available to the public any copyrighted material or other protected content where the security measure associated with a certified security technology has been removed or altered. Section 103 (b) provides an exemption to Section 103 (a) for time shifting purposes of programming at the time it is lawfully performed by a lawful recipient.

Section 104 (a) lists six criteria, which shall be applied to the development of security system standards and certified security technologies. Section 104 b through f provides for the respective administrative provisions concerning the development of such security standards under the surveillance of the Secretary of Commerce, who shall interfere, if representatives of interactive digital device manufacturers and representatives of copyright owners have not reached agreement on such standards within a period of 12 months after the date of enactment of the Bill and who shall initiate a rulemaking to adopt the standards.

According to Section 105 the Secretary shall certify technologies, that adhere to the security system standards adopted under Section 104, provided these technologies are available for licensing on reasonable and non discriminatory terms.

Section 108 provides for the application of Sections 1203 (civil remedies) and 1204 (criminal remedies) of the DMCA for violations of Sections 101 through 103 of this Bill.

⁹²⁴ See: Draft dated August 6th 2001 available under www.eff.org.

Section 109 finally provides for definitions of the key terms of the Bill. “*Interactive digital device means*” “*any machine, device, product, software or technology, whether or not included with or part of some other machine, device, product, software or technology, that is designed, marketed or used for the primary purpose of and that is capable of storing, retrieving, processing, performing, transmitting, receiving or copying information in digital form*”. “*Certified security technology*” means “*a security technology certified by the Secretary of Commerce under Section 105*”.

The Hollings Bill would therefore require any personal computer or any similar device like PDAs to incorporate security features designed to prevent unlawful uses, especially uses enabled by acts of piracy. The Hollings Bill would expressly provide for the so called “*no mandate*” rule, which had not been incorporated into the DMCA.

Since its introduction in the Senate of the United States of America there has been a very intensive discussion led by the content industries as promoters and the IT industry as opponents about this Bill. However at the end of 2002 it did not look as if its promoters and supporters were able to get this Bill enacted in the foreseeable future.⁹²⁵

V General Evaluation of the DMCA and the Hollings Bill Proposal

V.1 The Basics of Copyright Laws

By giving authors and owners of works protected under the Copyright Laws a set of strong additional rights to protect their works, Digital Rights Management and Copy Protection Systems touch the basic purposes of the Copyright Laws. Therefore before evaluating the DMCA and the Hollings Bill proposal, it is helpful to reconsider these purposes.

Copyright Laws must mediate between the specific interests of authors and the interests of the broader public. For their efforts in creating works sufficiently creative to be protected under the Copyright Laws authors may expect a remuneration by the country, in which such works have been created or in which they are to be used. Such remuneration lies in the protection of these works under the Copyright Laws, which gives the author (apart from certain moral rights⁹²⁶)

⁹²⁵ On March 21, 2002 Senator Hollings and other senators introduced the Consumer Broadband and Digital Television Promotion Act (CBDTPA), which like its predecessor, the Security Systems Standards and Certification Act would require all new hardware and software to block unauthorized copying of copyrighted works. Although the CBDTPA tried to address some of the criticisms directed at its predecessor, its general approach of prohibiting the distribution of any new hardware or software that does not include copy-protection schemes remains unchanged, confer to Intellectual Property & Technology Law Journal 2002, p.26/27.

⁹²⁶ By adherence to the Berne Convention the USA have accepted to protect the moral rights of attribution and integrity under Copyright Law, confer to the Berne Convention Implementation Act, Pub. L. 100-568, 102 Stat. 2853, 17 U.S.C.

exclusive rights in the economic exploitation of these works and by doing so in making profit. However the interests of the broader public require, that the protection of works under the Copyright Laws does not result in a perpetual monopoly concerning the work as such⁹²⁷ in order to develop and advance the public welfare. As stated in the WIPO Copyright Treaty, there is a “*need to maintain a balance between the rights of authors and the larger public interest, particularly education, research and access to information, as reflected in the Berne Convention.*”⁹²⁸ This particular balance requires on one side a strong set of exclusive rights, which protect the interests of the authors, but on the other side a number of limits and exceptions to these rights, which serve the interests of the broader public. While these rights and exceptions may vary from country to country, this basic principle is common ground under most Copyright Laws.

V.2 The Effects of the DMCA and the Hollings Bill Proposal on the Basics of Copyright Laws According to Voices in the Legal Community in the USA

In Regards to the DMCA

Most of the critics in the academic world in the United States consider the balance between rights of authors/copyright owners and rights of the broader public to be violated in favour of the authors/copyright owners.⁹²⁹ The following arguments are mentioned in this context:

The circumvention prohibition in Section 1201 (a) (1) is considered to be too broad, because it prevents any circumvention, including circumventions, which are performed for lawful purposes, f.i. for the purposes of fair use.⁹³⁰ According to these voices the circumvention prohibition should have been limited to acts, which have to be considered as infringements of the authors/copyright owners rights. The proponents of this opinion argue with Art. 11 of the WIPO Copyright Treaty, which does not require the broad solution taken by the DMCA, but requires only such legal remedies against the circumvention of effective technological measures, that restrict acts, which are not authorised by the right holders.

Another major objection against the DMCA concerns the exceptions. It is especially criticised, that Section 1201 (a) 2 and (3) do not allow the marketing of devices, which are designed to enforce the exceptions covered under Section 1201 c-f. Therefore some of these exceptions run dry, because without help from other

⁹²⁷ That is the reason, why Copyright Laws (other than the Patent Laws) do not protect the ideas behind the individual work, but protect only the expression of such ideas, so called idea/expression dichotomy.

⁹²⁸ See: WIPO Copyright Treaty, Preamble; Vinje (1999): 193.

⁹²⁹ See: Samuelson (1999); Fn. 909: p. 534; Nimmer (2000). Fn. 909: p. 740/741. Ginsburg (2000): 12; Unintended Consequences, three years under the DMCA, Comments of the Electronic Frontier Foundation, dated May 3d 2002, available at: www.eff.org.

⁹³⁰ See: Samuelson (2000); Fn. 909: p. 543 and 546; Benkler (1999): 415.

people and the use of respective devices, only those very few individuals being extremely familiar with the computer and software technology will effectively be able to take benefit from these exceptions.⁹³¹

A third concern is the effect of the DMCA on the “fair use” doctrine. Although as explained above, the courts have decided, the DMCA would not violate the “fair use” doctrine, voices⁹³² in the academic legal community believe, that the DMCA does in fact restrict the rights of any user under the “fair use” doctrine to an unacceptable extent.

Finally commentators⁹³³ do not agree with the court rulings insofar as an eventual violation by the DMCA of the First Amendment is concerned.

In Regards to the Hollings Bill Proposal

The Hollings Bill proposal would finally lead to ultimate control of the IT industry over the user of computer and software products. Already major industrial players like Intel and Microsoft have announced to work on “trusted systems”,⁹³⁴ which would require the user of a computer system to rely on components, which have been approved by the manufacturer or the hardware and software.⁹³⁵

All those concerns, which are raised against the DMCA apply here as well. However as the Hollings Bill does not provide for any exceptions, the concerns against the DMCA would apply to a much larger extent. Especially the fact, that no exception for reverse engineering, comparable to Section 1201 (f) of the DMCA is given, would definitely raise a lot of concern,⁹³⁶ unless such exception as well as others would be agreed upon by the representatives of the manufacturers and those of the copyright owners in the agreements to be concluded by the two group to determine the security standards according to Section 104 Hollings Bill proposal.

In the meantime even parts of the content industries seem to turn away from the concept of copy protection systems to be introduced by mandatory laws. On January 14 th 2003 the Recording Industry Association of America (RIAA) together with the Business Software Alliance (BSA) and the Computer Systems Policy Project (PSPP) published a position paper, which raises concerns against any regulation of copy protection requirements comparable to the Hollings Bill by statutory laws. It is interesting to note, that the movie industry does not share this initiative.⁹³⁷

⁹³¹ Confer to the examples at Nimmer (2000); Fn. 909: p. 737; Samuelson (1999); Fn. 909: p. 548, 551; Benkler (1999); Fn. 930: p. 415.

⁹³² See: Fn. 929.

⁹³³ See: Benkler (1999); Samuelson (1999); Fn. 931.

⁹³⁴ See: Gimbel (1998): 1674.

⁹³⁵ See:

www.microsoft.com/presspass/press/2003/Jan03/01-20SessionToolkitPR.asp.

⁹³⁶ Concerning the issue of reverse engineering confer to Vinje (1996): 442.

⁹³⁷ See: <http://online.wsj.com/article/0,,SB1042509178176423064,00.html>.

V.3 Evaluation of the DMCA and the Hollings Bill Proposal by the Author of This Article

From my point of view, the discussions around the DMCA very clearly show the dilemma,⁹³⁸ which the lawmaker, who needs to adjust the Copyright Laws to the new challenges of the digital era, has to face.

On one side the content owners and that means especially the Entertainment industries need to make sure, that they will survive in the digital age, where it is possible to copy any movie or piece of music with any standard PC by a simple maus-click. Napster and other similar enterprises have seriously endangered the music industry, which, other than the movie industry by applying the CSS technology to DVD products right from he start, has never provided any copy protection until technologies like Napster and others forced them to do so in order to survive. But even the movie industry had to face the fact, that software, which make the CSS technology ineffective, can simply be downloaded from the web in a few seconds of time. Therefore for the survival of these industries effective copy protection systems, which enjoy the protection of the laws are a “must” to survive.

On the other hand users of copyrighted works want to be able to use digital products to the same extent as analog products. Copying movies for time shifting purposes or copying music for private collections not to be used in any business are legitimate purposes, which the lawmaker should support. One point, which needs to be calculated in, is the fact, that the content owners are big companies, which are very powerful, whereas the typical user, as a private consumer, is very weak.

Therefore the lawmaker is “put between a hard rock and a stone”. If the laws give the content owners strong rights, these industries will survive, but the user rights will suffer. If the lawmaker gives the user more rights and exceptions to the rights granted to the content owners, this may allow hackers and people with similar minds to use such rights and exceptions for the purpose of circumvention. Once a circumvention has successfully been achieved and a respective software like the DeCSS software has been put on the world wide web, it is extremely difficult, to prevent people from using such software. Even if the content owner would win a law suit in the United States of America against the “Hacker”, the software would long have been put on a server located in some other country of the world at the time of a judgement in the USA, and this “game” would continue, even if the content owner would also sue in that country. Therefore the “ubiquity” of the Internet makes things worse and as long as we do not have solutions for the world wide enforcement of “Internet based Piracy” this will not change.⁹³⁹

Based on these thoughts, it is my impression, that the lawmaker of the United States of America by enacting the DMCA has provided legal rules, safe enough to guarantee the survival of the Entertainment industries. Apparently the rights

⁹³⁸ See: Gladney (2000): 55; Vinje (1999); Fn. 928: p. 197.

⁹³⁹ See: Gimbel (1998); Fn. 934: p. 1674.

of users suffer, because in order to have effective anti-circumvention rules, the exceptions were tailored narrow, probably too narrow. However the DMCA requires the Librarian of Congress to report to Congress any three years whether users are adversely affected by the prohibitions of Section 1201 (A) of the DMCA in their ability to make non infringing uses of copyrighted works. Therefore the lawmaker has provided for a “loophole”, which enables him to initiate corrections to the DMCA in favour of user rights.⁹⁴⁰ Overall this concept seems to be appropriate, even if details may not fit.

Concerning the Hollings Bill proposal, the discussion held in the USA is strange. On the one hand the manufacturers of PC systems and other hardware fight the proposal rigorously. On the other hand Intel and Microsoft have announced to develop “trusted systems” on their own,⁹⁴¹ which would finally have a similar effect than the Hollings Bill. The impression cannot be avoided, that the big manufacturers do not fear the content of the Hollings Bill, but the fact, that the Hollings Bill would take their independence in developing such security features by requiring them to agree on these features with the representatives of the content owners. It could therefore happen, that security features as required by the Hollings Bill proposal will be introduced in recent future anyhow by private initiative of major IT companies. However as already mentioned above, this will bring new questions on the table concerning user rights, such as the question of “reverse engineering”, “first sale doctrine”, “back-up copies”.⁹⁴² Any guidelines, how these issues could be solved are missing in the Hollings Bill proposal and its successor, the CBDTPA.⁹⁴³

V.4 Comparison with the EU Directive on the Harmonisation of certain Aspects of Copyright Law, EU 2001/29⁹⁴⁴

Among other aspects, the EU directive on the harmonisation of certain aspects of copyright law provides a legal framework for the member countries to introduce rules and regulations concerning Copy Protection and Digital Rights Management Systems into the national laws.

However there is one basic difference in Europe compared to the USA. In Europe there is a long tradition of levies to be paid to the collecting societies as representatives of authors on analog products as remuneration for certain rights of

⁹⁴⁰ See: Samuelson (1999); Fn. 909: p. 560, sceptical about the effectivity of this procedere.

⁹⁴¹ The Trusted Computing Platform Alliance guided by Intel and Microsoft has developed a computer chip, which would be integrated directly on the motherboard of the computer. The chip would encrypt data already on the hardware level, thus giving absolute control, confer to “www.golem.de/0210/22234.html”, confer also to the Microsoft press statement referenced under note 934. See also: *Kuhlmann, Gehring* within this book on page 178.

⁹⁴² According to Gimbel (1998); Fn. 934: p. 1685 the whole issue of anti-circumvention rules in the DMCA has to be seen in the context of mass market licenses.

⁹⁴³ See: Fn. 926.

⁹⁴⁴ See: Fn. 898.

users to copy copyrighted materials for private purposes. This levy scheme is all but uniform and varies from country to country; some countries put levies only on media, others put levies on hardware products like VCR systems, others put levies on both. During the last few years an intensive debate has started concerning levies on digital products, like scanners, CD burners, PC systems and printers. It is too early to say, how this debate will finally end up, but it seems as if levies for certain digital products will be introduced for an intermediate period, until Digital Rights Management Systems will be generally available. As mentioned above, the Audio Home Recording Act of the USA does not provide for levies on such kind of digital products like PC Systems and to the best of my knowledge there is at present no discussion held in the USA to change the current procedure.⁹⁴⁵

What we learn from this, is that within the EU apparently DRM and Copy Protection Systems do not enjoy the same trust by content owners and collecting societies as they do in the USA. DRM Systems will eventually be introduced in Europe in coexistence with levies on certain digital products.

Art. 6 I of the EU directive requires the member countries of the EU to provide for adequate legal protection of efficient technical anti-circumvention measures, but leaves any details on how such protection shall be implemented into the national laws of the member countries to the discretion of such countries. This approach provides for more flexible solutions, which allows to adjust to the specific situation in each country. However similar problems as in the USA may eventually arise, as can be seen in Germany. Art. 53 of the German Copyright Act expressly allows to make certain copies of copyrighted materials for private purposes. The proposal of the German government for the implementation of the EU directive into German law⁹⁴⁶ formally retains such rights, but on the other hand establishes legal protection to right holders using anti-circumvention technologies in Sections 95 a through c of the implementation Bill proposal. Sections 95 a through c declare it illegal (i) to interfere with copy protection measures/systems or to make such measures/systems ineffective and (ii) to market or import devices designed to interfere with or make copy protection measures/systems ineffective. Therefore the rights of users according to Section 53 German Copyright Act will run dry, if content owners generally do apply such copy protection measures/systems in the future. The music industry has already adopted such copy protection measures by technically preventing Compact CDs to be copied using a PC system. The public debate in Germany about this issue has begun, but will eventually be less intensive than in the USA as long as no proposal comparable to the Hollings Bill will be put on the table.

Therefore although the EU directive does not mandate any specific anti-circumvention rules and provides to the member countries a certain extent of “freedom of implementation”, the discussion on user rights and exceptions is a major topic in Europe as well.⁹⁴⁷

⁹⁴⁵ Concerning the collecting societies in the USA confer to Goldmann (2001b).

⁹⁴⁶ Available at: www.bund.bmj.de.

VI Conclusion

The modern technologies make our daily lives easier; nowadays contracts for almost all kind of businesses can be concluded by a simple maus-click. However the more easy it is to use the capabilities of the modern technologies, the more difficult it seems for the lawmaker to implement laws and regulations, which keep the balance of copyright laws alive. The technical “revolution” will continue, so will the difficulties for the lawmakers to adjust the legal framework to such developments.

⁹⁴⁷ See also: *Dreier* (page 479); *Goldmann* (page 502); *Günnewig* (page 528); *Reinbothe* (page 405) within this book.

4.1.2 The Copyright Wars — A Computer Scientist’s View of Copyright in the U.S.

Barbara Simons⁹⁴⁸

Congress shall have the power [...] To promote the progress of science and the useful arts, by securing for limited times to authors and inventors the exclusive rights to their respective writings and discoveries.

United States Constitution, Article I, Section 8

I Introduction

Copyright is an area that until recently was of interest primarily to intellectual property (IP) lawyers and law professors. As a computer scientist and a non-lawyer whose only interactions with IP lawyers until the past decade involved applying for patents, I was convinced that IP law was among the most boring of topics. I now find it fascinating, a change that was brought about by the clash of technology, politics, and the law.

There were two forces that combined to move copyright from the realm of a few specialists to a topic that appears frequently on the front pages or in the business sections of newspapers. Those forces are the development of digital technology and the growth of the internet. The relevance of “digital technology” is that information, including movies, songs, and books, is now stored as a string of 0’s and 1’s, otherwise known as “bits”. A string of 0’s and 1’s is easy to copy, and each copy is identical to every other one — in other words, a perfect copy. By contrast, each time a document is photocopied or a movie videotaped using non-digital technology, the new copy is not quite as good as the one being copied. Also, each photocopied page costs a few pennies, and each new videotape has an initial cost of the purchase price of a blank tape. But digital copies are essentially free, so long as the required storage or net access is available. Consequently, the disincentives of deteriorating quality together with cost do not apply to the production of massive numbers of digital copies.

The internet has provided a vehicle for the widespread and essentially free distribution of digital copies, although some limitations remain. Movies, in particular, are still too large for most people to download in any reasonable period of time. However, as bandwidth and speed increase, it’s likely that the time required to download a movie will not be a major impediment within a few years.

Not surprisingly, the movie and record industries feel threatened by the digital revolution. Napster, which was a centralized system, and peer-to-peer (P2P) systems such as KaZaA, Morpheus, and Grokster make it possible to download specific songs without paying for them. Since the technology for burning a CD is widely available, it’s now possible for people to create customized CDs that contain only the music they want to hear.

⁹⁴⁸ U.S. Public Policy Committee of the Association for Computing Machinery (USACM).

Consequently, the movie and record industries are pressuring Congress and the courts to eliminate “piracy”, the term that content owners tend to use for unauthorized copying of copyrighted material. Not only is “piracy” a loaded word, given that pirates of old were inclined to steal, rape, and murder, but it also clouds the fact that, because of fair use and other restrictions on copyright, unauthorized copying is not necessarily illegal⁹⁴⁹. Indeed, there appears to be a power grab on the part of the content industries to make all unauthorized copying illegal. Sometimes this argument can be rather torturous, as is illustrated in the discussion of the Digital Millennium Copyright Act (see below) in the paper by Dr. Mathias Lejeune within this book on page 366. He notes that the law does not prohibit the act of circumventing technological measures that prevent copying, thereby, presumably, retaining fair use⁹⁵⁰ rights. But he then goes on to say that circumventing to gain unauthorized access to a work is illegal. I leave it as an exercise for the reader to determine how a person can exercise his or her fair use rights without gaining access to a work.

It’s difficult to determine how much the music industry has been damaged by the downloading of music from the internet. The industry tends to blame “piracy” for drops in sales, as the following quote⁹⁵¹ from the BBC illustrates:

[T]otal U.S. music shipments dropped 10.1% from 442.8 million units in the first half of 2001 to 398.1 million units in the first half of 2002. This meant sales dropped 6.7% in the U.S., from \$5.93bn in the first half of 2001 to \$5.53bn in the first half of 2002. Record company bosses are adamant this drop can be explained by music “piracy”, despite the correlation with the downturn in America.

In addition to the negative impact of the economic downturn on music sales, spokespeople for the music industry tend to ignore the fact that some people who download songs from the internet eventually purchase the CDs containing those songs. Determining how many people make legal purchases after downloading music from a P2P system versus the number of people who no longer purchase music that they can obtain for free via the internet is an impossible task. Still, it’s reasonable to assume that the music industry has been hurt financially by the availability of free copies of the music.

The question is how to deal with the economic effects of the digital revolution on content providers. While there have been some efforts on the part of the music industry to develop business models that exploit the internet, these efforts have not been particularly successful. Obviously, they are not yet offering people what they want and are willing to pay for⁹⁵².

⁹⁴⁹ In this document I shall use more precise words like “infringing” and “unauthorized” rather than “piracy” except when referring to the language of others.

⁹⁵⁰ Fair use is similar to the notion of “fair dealing” in the UK and several other English speaking countries.

⁹⁵¹ See: <http://news.bbc.co.uk/1/hi/entertainment/music/2218860.stm>.

⁹⁵² There have been some interesting new business models introduced recently. One that is getting a lot of attention and has far exceeded initial expectations is Apple’s “iTunes Music Store”, which is selling music at \$0.99 per song.

Creating genuinely new business models is risky, and there is a disincentive to take risks when the current business model is successful. Consequently, most of the efforts of the movie and record industries have been devoted to the passage of new laws and to the prosecution of test cases under both old and new laws. Below I discuss relevant laws and legal proposals, as well as some interesting court cases. A key component of the discussion is the negative and perhaps unanticipated impact that laws designed to protect the economic interests of the movie and record industries are having on the rest of us, independent of whether we've ever downloaded any digital material from the internet.

I.1 A Little History

Prior to the passage of the Copyright Act of 1709, also known as the Statute of Queen Anne⁹⁵³, British law did not recognize the rights of authors and creators; documents could be published without compensating the author. The Copyright Act of 1709 gave new works fourteen years protection, renewable for another fourteen years if the author was still alive. At the end of that time, the work entered the public domain.

The influence of British law is reflected in the Copyright Clause of the U.S. Constitution, which empowers Congress to provide a limited monopoly to creators in order to encourage and reward creativity. But there is a natural progression: once the monopoly expires, the creation becomes a part of the public domain and is available to all. This is intended to benefit the general public, including creators, who can then build on the work of others.

An interesting historical footnote, especially in light of the accusations for “piracy” leveled by several U.S. content producers at some other countries, is that in the nineteenth century the U.S. was a haven of “piracy”. For example, translations of a copyrighted work were not considered protected by copyright in the U.S. until 1870; a German translation of *Uncle Tom's Cabin* was determined in 1853 not to be covered by copyright. International protection for copyright was not provided in the U.S. until 1891, something that greatly irritated Charles Dickens, whose works were published in America for a fraction of what they cost in the UK.

Many laws have been passed and cases litigated since the early days of copyright. We shall be focusing on recent court cases and modifications to copyright law, especially since digital technology and the Internet have become major forces in our society.

I.2 Length of Copyright

In 1790 Congress passed the first Copyright Act, which provided the same term for copyright as the Statute of Queen Anne. The term of copyright was length-

There are copying limitations, but they appear to be designed primarily to prevent illegal commercial copying, as opposed to copying done by individuals for personal use. See: <http://www.apple.com/music/store/>.

⁹⁵³ See: <http://press-pubs.uchicago.edu/founders/documents/a1.8.8s2.html>.

ened in 1831 to a base term of 28 years and a second 14 year renewal, giving a maximum total of 56 years. Additional extensions made during the earlier part of the twentieth century culminated in the Copyright Act of 1976, which created a term of copyright consisting of the author's life plus fifty years or 75 years for "works for hire" or anonymous works. None of the extensions covered works that had already entered the public domain.

A bit more than twenty years after the passage of the Copyright Act of 1976, Congress passed the Sony Bono Copyright Term Extension Act (CTEA) of 1998. The CTEA, which applied retroactively to materials that had fallen out of copyright, extended protection to 70 years beyond the life of the creator and, for works for hire the shorter of 95 years from the first publication and 120 years from creation. The twenty year increase has lead some to rename the 1998 legislation as the "Mickey Mouse Extension Act," since the copyright on Mickey Mouse would have expired in 2003 had the extension not existed.

1.3 User Rights under Copyright in the United States

While copyright is a monopoly, it is not an absolute monopoly, and unauthorized copying is not necessarily illegal. Under first sale doctrine, I can destroy, resell, or give my copy of a copyrighted work to someone else without first obtaining permission of the copyright holder. About a century ago book publishers attempted to undercut the first sale doctrine by including a license in each new book that obligated the purchaser to resell the book at its original cost. The Supreme Court ruled in a 1908 case (*Bobbs-Merrill Co. v. Straus*) that the licensing scheme was illegal, because the exclusive right to sell a copyrighted work applies only to the first sale of that work. It's interesting to conjecture as to whether or not first sale doctrine will eventually be applied to copyrighted software. When you purchase software, do you really just buy a license, or do you actually purchase a copy, much as you do with a book?

Another important user right is fair use. The fair use doctrine, which was incorporated into the 1976 Copyright Act, states that copying "for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright." The fair use doctrine applies to all copyrighted material, not just printed documents.

Fair use is not rigorously defined in U.S. law, which is why there have been court cases testing whether or not a particular type or incidence of copying is protected under fair use. Therefore, it is impossible to devise algorithms or heuristics that directly implement fair use, a problem confronting many digital rights management (DRM) developers. An open question is whether or not it is possible to develop a policy that would protect fair use under some DRM scheme, for example by allowing the user to declare that fair use allows him or her to copy a portion of a copyrighted document, without violating the user's privacy. If DRM becomes widely deployed without adequate protection for fair use, the result will be legislation by technology. Not only is this contrary to the

democratic principle, but also it would hinder or even eliminate a user right that has been developed over an extended period of time.

DRM threatens to upset the previous balance of creator and user rights contained in copyright law by making it difficult to impossible both to exercise fair use rights and to produce an unscrambled version of a work for the public domain once copyright has expired. These problems are exacerbated by some recent and proposed legislation.

II Laws and Legislative Proposals

While debate on new copyright legislation triggered by the digital revolution began around 1994⁹⁵⁴, the first relevant law was not passed until 1997.

II.1 The No Electronic Theft Act (NET)⁹⁵⁵: An Early Response to the Internet

The NET Act, signed into law by President Clinton on Dec. 16, 1997, criminalizes the electronic distribution of copyrighted material, even if there is no financial gain, so long as the total retail value of the material is at least \$1000 during a distribution period of 180 days. The penalty is up to one year in prison and a fine of up to \$100,000 — unless the total retail value is over \$2500. In this case, the violation jumps from a misdemeanor to a felony, a conviction for which can result in up to three years imprisonment and a fine of up to \$250,000.

A major issue with the NET Act is determining the total retail value of material that is downloaded from the internet. For example, suppose Alice accesses my website and downloads this article onto her computer. Does that access count towards the total retail value? What if Alice reads only one or two sentences before getting bored and deleting my article? Should that also count? Suppose Bob's machine crashes while he is reading my article and he is so fascinated by it that he accesses my article again after rebooting. Should that second access also be counted?

Assume that I had posted a copy of Windows 3.1 on my website. Is the retail value of a single copy the price for which Windows 3.1 was sold when it was released? Is it the price for which it could be sold now?

In 1990, a copy of Bell South's manual on the 911 system appeared in an online magazine (e-zine) called Phrack, published by Craig Neidorf. Although the Bell South document was obtained by someone else from Bell South's computer, Neidorf was charged with wire fraud on the grounds that the 911 manual had a

⁹⁵⁴ Bruce Lehman, Assistant Secretary of Commerce and Commissioner of Patents and Trademarks, chaired the Working Group on Intellectual Property Rights of the Information Infrastructure Task Force. In 1994 the Working Group issued its Green Paper. Lehman's Nov. 15, 1995 Congressional testimony on a precursor to the DMCA can be found at: <http://www.uspto.gov/web/offices/com/doc/ipnii/nii-hill.html>.

⁹⁵⁵ See: <http://www.usdoj.gov/criminal/cybercrime/17-18red.htm>.

value of \$79,449. The value of the manual was a critical component of the case, since the law required that the stolen property be worth at least \$5000. The government dropped all charges when it was revealed in court that the same document was being sold by Bell South for \$13. While Neidorf was spared a potential prison term of up to 65 years, he was left with a \$100,000 legal bill.

There have been very few convictions under the NET Act, and it has received far less attention in recent years than the more recently passed and controversial Digital Millennium Copyright Act.

II.2 The Digital Millennium Copyright Act (DMCA)⁹⁵⁶

The DMCA was enacted in 1998 to implement a World Intellectual Property Organization Copyright Treaty⁹⁵⁷. Copyright experts such as Prof. Pamela Samuelson, claimed that U.S. law already was adequate⁹⁵⁸, but the content industry was eager for the passage of strong legislation that they felt would protect their products. Since the DMCA criminalizes technologies and technological devices, rather than infringing behavior, it's primarily an anti-technology law, as opposed to a copyright law.

Two aspects of the DMCA that have proven especially problematic to computer scientists are the anti-circumvention and anti-dissemination provisions. The anti-circumvention provision makes it illegal to “*circumvent a technological measure that effectively controls access to a work*”. The anti-dissemination provision makes it is illegal to “*manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that (A) is primarily designed [...] for the purpose of circumventing a technological measure that effectively controls access to a [protected] work [...], (B) that has only omitted commercially significant purpose or use other than to circumvent [...], or (C) is marketed [...] for use in circumventing a technological measure [...]*”.

One of the interesting aspects of the DMCA is the effort made by policy makers to give legal definitions for technological notions: “*(A) to ‘circumvent a technological measure’ means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner; and (B) a technological measure ‘effectively controls access to a work’ if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work*”.

The definition of effectively controlling access to a work is vague at best. There is no definition of what effective, as opposed to ineffective, means. How weak would a scrambling (encryption) scheme need to be in order to be viewed as not effective? Would a “cereal box” level encryption that permutes the letters of

⁹⁵⁶ See: <http://www.gseis.ucla.edu/iclp/dmca1.htm>.

⁹⁵⁷ See: <http://www.wipo.org/eng/diplconf/distrib/treaty01.htm>.

⁹⁵⁸ See: <http://www.firstmonday.dk/issues/issue4/samuelson/>.

the alphabet be effective? What about a 40-bit scheme that can be broken (decrypted) easily by trying all possibilities (exhaustive search)? Would the Navajo language, which was used as a kind of encryption by the U.S. during WWII, qualify as an effective measure? Who decides?

Well, of course, the courts decide, as we discuss below.

The DMCA contains the following exceptions to the anti-circumvention and anti-dissemination provisions: reverse engineering for interoperability, encryption research, preventing minors from accessing material on the Internet, privacy protection, and security testing. However, even these exceptions are quite limited. For example, in order to qualify for the encryption research exemption, one must be “*engaged in a legitimate course of study, employed, or appropriately trained or experienced, in the field of encryption technology*”. It appears that even a research mathematician or computer scientist who is not labeled as an encryption researcher may not qualify for the encryption exemption. (See the discussion of the Felten et al. case below). Similarly, in order to qualify for the security exemption, one must have “*the authorization of the owner or operator*” of the computer, computer system, or network.

One of the many ironies of the DMCA is that it claims to protect fair use rights. But given the anti-circumvention and anti-dissemination provisions of the law, there is no legal way to exercise one's fair use rights if a work is protected by an “effective” (or even ineffective) technological measure.

While probably not the intent of the drafters of the DMCA, the DMCA also has the effect of criminalizing a number of techniques, such as penetration analysis and reverse engineering for virus detection, that are used by computer security experts⁹⁵⁹. This is because it's not possible in general to prove that a large complex system is secure, and so people are reduced to attempting to break the system — something that could be illegal under the DMCA.

There was, however, some awareness on the part of the drafters of the DMCA that the anti-circumvention and anti-dissemination provisions, the implementations of which were delayed until 2000, would inhibit the kind of reverse engineering required to fix the Y2K problem⁹⁶⁰. Either the drafters of the DMCA felt that Y2K was the only situation in which there is a valid need to reverse engineer copyrighted software, or they were indifferent to the existence of other legitimate reasons for reverse engineering software.

Until recently, copyright laws tended to stipulate only civil penalties. The DMCA, like the NET Act, contains criminal as well as civil penalties. Circumvention of “copyright protection” or of “integrity of copyright management information” for commercial advantage or private financial gain can be penalized

⁹⁵⁹ An excellent letter signed by forty-nine computer security experts on the risks posed by the DMCA can be found at:
<http://www.cerias.purdue.edu/homes/spaf/WIPO/index.html>.

⁹⁶⁰ My suspicion that implementation was delayed because of Y2K was confirmed in a private conversation with a former House staff person who had been involved with some of the committee work relating to the legislation.

with a fine of up to \$500,000 or five years in prison or both for the first offense; the penalties can double for subsequent offenses.

The Digital Era Copyright Enhancement Act⁹⁶¹, introduced by Boucher (D-Va) and Campbell (R-Ca), was proposed as an alternative to the DMCA. The Campbell/Boucher bill would have prohibited altering or deleting copyright management information *for the purposes of infringement*. By contrast, infringement need not occur for someone to be found guilty under the DMCA. Campbell/Boucher also would have prohibited enforcement of terms in shrink-wrap and click-through agreements or licenses when they reduce privileges recognized by copyright law. The proposed legislation had only civil penalties, not criminal. Hollywood and the record industry strongly supported the DMCA and opposed the Campbell/Boucher bill. In spite of concerns expressed by academics, librarians, and computer security experts relating to fair use and computer security, the DMCA became law.

II.3 The Consumer Broadband and Digital Television Promotion Act (CBDTPA)⁹⁶²

The CBDTPA was introduced March 22, 2002 by Sen. Fritz Hollings (D-NC), Sen. Diane Feinstein (D-Ca), Sen. Ted Stevens (R-Al), Sen. Daniel Inouye (D-Hi), Sen. John Breaux (D-La), and Sen. Bill Nelson (D-Fl). It was a follow-on legislative proposal to the Security Systems Standards and Certification Act⁹⁶³ (SSSCA) that was circulated, but never introduced, by Sen. Hollings. The primary goal of both the SSSCA and the CBDTPA is to control copyright violations via some mechanism built into the hardware and software. The thinking behind the CBDTPA is summarized by the following quote from Michael Eisner, CEO of Disney, at a Congressional hearing on February 28, 2002.

“[D]igital technologies can enable a level of piracy — theft — that would undermine our capacity to produce films and entertainment, undermine the deployment of Broadband networks, undermine the digital television transition and ultimately result in fewer choices and options for American consumers.”

The proponents of the CBDTPA claim that broadband will not be extensively deployed until there is a “killer app”, in this case movies over the Internet. The movie studios state that they will not make movies available via broadband until they feel confident that the movies will not be copied without permission. As Eisner said at the same Congressional hearing:

“[O]nce standards [for digital rights management] are set, they must be mandated for inclusion in all digital media devices that handle creative content. This is necessary to ensure a reasonably secure environment and to prevent unfair competition by non-compliant device manufacturers.”

⁹⁶¹ See: <http://www.arl.org/info/frn/copy/bouch.html>.

⁹⁶² See: <http://cryptome.org/broadbandits.htm>.

⁹⁶³ See: <http://cryptome.org/sssc.htm>.

Under the CBDTPA: “A manufacturer, importer, or seller of digital media devices may not

- (1) sell, or offer for sale, in interstate commerce, or
- (2) cause to be transported in, or in a manner affecting, interstate commerce, a digital media device unless the device includes and utilizes standard security technologies that adhere to the [adopted] security system standards.”

In addition: “No person may knowingly apply to a copyrighted work, that has been distributed to the public, a security measure that uses a standard security technology in violation of the [adopted] encoding rules.”

The CBDTPA would apply to any digital media device, where a digital media device is defined to be: “any hardware or software that —

- (A) reproduces copyrighted works in digital form;
- (B) converts copyrighted works in digital form into a form whereby the images and sounds are visible or audible; or
- (C) retrieves or accesses copyrighted works in digital form and transfers or makes available for transfer such works to hardware or software described in subparagraph (B).”

The CBDTPA contains anti-circumvention and anti-disseminations rules, as well as the same criminal penalties as the DMCA. Security measures would be agreed on by industry or, failing that, by government mandate; statutory damages of \$200 – \$2500 would apply for any non-compliant security measure used for a copyrighted work being distributed to the public.

There are many obvious problems with the CBDTPA. As is the case with the DMCA, the CBDTPA would criminalize some standard computer security technologies, rather than criminalize infringing behavior. Since there is no way to distinguish protected content from personal or public domain material, legitimate and important code distribution could be inhibited. If internationally disseminated free/open systems such as Linux, GNU⁹⁶⁴, and FreeBSD do not incorporate the copyright detection mechanism mandated by the U.S. government, these systems could be crippled or even eliminated.

The CBDTPA raises more questions than it answers. Would it be legal to teach students to write a simple program that reads an input and then prints it out? Would it be possible to distribute urgent software patches? Could open/free software be legally distributed for educational and research uses? What would be the impact on personal and political speech as well as the ability to conduct free on-line performances?

Perhaps most significant is that the inclusion of anti-copying technology in general purpose equipment, as mandated by the CBDTPA, would add complexity and the potential for failure to critical real-time computing devices used in traffic control, air flight control, medical equipment, and manufacturing. The

⁹⁶⁴ Such a refusal is almost a certainty, at least for GNU. See for example <http://www.gnu.org/philosophy/can-you-trust.html> in which Richard Stallman refers to the CBDTPA as “the Consume But Don't Try Programming Act”.

complexity increases the risk of unexpected interactions with other code, as well as accidental activation of some emergency protocols.

II.4 Legislative Proposals to Reduce the Scope of the DMCA

Two bills were introduced in the House of Representatives in October 2002 that would limit some aspects of the DMCA. The first, the Digital Choice and Freedom Act of 2002⁹⁶⁵ (Lofgren D-Ca), would guarantee first sale rights and allow consumers to make backup copies. It would also permit circumvention of content protection technologies to make non-infringing copies and allow dissemination of circumvention technologies that enable non-infringing use if the copyright owner has not provided such a capability. A day later the Digital Media Consumers' Rights Act⁹⁶⁶ (Boucher D-Va, Doolittle R-Ca) was introduced. It also would allow circumvention of copy protection mechanisms for non-infringing uses and dissemination of technologies "capable of enabling significant noninfringing use of a copyrighted work". In addition, it would require copy-protected CDs to include "prominent and plainly legible" notice if anti-piracy technology could make them unreadable on some CD players. The Boucher/Doolittle bill was reintroduced Jan. 8, 2003 as H.R. 107, and the Lofgren bill, renamed the BALANCE Act of 2003, was reintroduced March 4, 2003 as H.R. 1066.

While neither bill is likely to pass in 2003, their introduction may signal the beginning of a Congressional debate on some of the problems created by the DMCA's approach of criminalizing technologies instead of behavior.

II.5 The Peer-to-Peer (P2P) Piracy Prevention Act⁹⁶⁷

On July 25, 2002 Rep. Howard Berman (D-Ca), together with Rep. Howard Coble (R-NC), Rep. Lamar Smith (R-Tx), and Rep. Robert Wexler (D-Fl), introduced legislation that would protect copyright owners from "any criminal or civil action for disabling, interfering with, blocking, diverting, or otherwise impairing the unauthorized distribution, display, performance, or reproduction of his or her copyrighted work on a publicly accessible peer-to-peer file trading network, if such impairment does not, without authorization, alter, delete, or otherwise impair the integrity of any computer file or data residing on the computer of a file trader". The legislation uses the word "unauthorized" (as opposed to "infringing"), even though fair use does not require that a work be authorized in order to be legally copied. As a result, unauthorized but legally posted works would be at risk if this legislation were to become law. The legislation would grant immunity from all laws, state and federal, civil and criminal, to copyright owners and their agents in their efforts to stop unauthorized distribution of their products. Finally, there is no requirement that the copyright holder give notice to

⁹⁶⁵ See: http://www.house.gov/lofgren/press/107press/021002_act.htm.

⁹⁶⁶ See:

<http://www.techlawjournal.com/cong107/copyright/boucher/20021003bill.asp>.

⁹⁶⁷ See: <http://www.house.gov/berman/p2p.pdf>.

the P2P network owner, nor is there any requirement that the copyright holder provide evidence of illegal behavior on the part of the P2P owner.

If “wrongful impairment” caused by a copyright owner resulted in at least \$250 in economic loss⁹⁶⁸ to a P2P network, a network owner wishing to be compensated must initially file a claim with the Attorney General of the United States. The network owner must then initiate a court action within 60 days after one of two things happened: 1) the Attorney General makes a determination or 2) 120 days have passed during which the Attorney General made no determination.

The copyright owner loses protection against legal action if he or she causes a loss greater than “\$50 per impairment” to the owner of the P2P network, beyond the economic loss associated with disabling access to the copyrighted work. It’s not clear, however, what, if any, penalties would apply to a copyright owner who exceeded the \$50 per impairment limitation, nor even in many cases how the P2P network operator would prove a such loss.

In a letter to Rep. Coble⁹⁶⁹, USACM, which is the U.S. Public Policy Committee of the Association for Computing Machinery (ACM), raised the following concerns:

- The definition of a “peer-to-peer public network” seems to include all computers connected to the Internet as well as fundamental software applications such as email and WWW service.
- Legally encouraged interdiction, spoofing, redirection, and denial-of-service attacks would create new volumes of network traffic resulting in Internet service disruptions and degradation of service for innocent Internet users, many of whom may not be using P2P networks. Such uses include electronic commerce transactions and a variety of research, education, free speech, health care, and other noncommercial activities.
- The legislation underestimates the technical challenge in targeting an attack at a specific copyrighted work without causing collateral damage to others through a shared connection, server, or repository of personal and business files.
- Legally sanctioned attacks would involve defeating legitimate security mechanisms and firewalls. This approach conflicts with efforts to enhance cybersecurity and seems to violate the anticircumvention provisions of the Digital Millennium Copyright Act and prohibitions in the USA Patriot Act.
- The legislation does not recognize that P2P networking protocols are used for a variety of purposes. Research and development conducted using P2P shows great promise for inexpensive yet powerful distributed computation.

The P2P legislation has been quite controversial within the technical community, where some refer to it as a “vigilante” bill. As of this writing, it has not been reintroduced in 2003.

⁹⁶⁸ Only monetary loss is allowed. Unpaid time required to repair damage to a system would not be counted as a loss.

⁹⁶⁹ See: <http://www.acm.org/usacm/Letters/P2P.htm>.

II.6 Anticounterfeiting Amendments of 2002⁹⁷⁰

Introduced on April 30, 2002 by Sen. Joseph Biden (D-De), the goal of the anticounterfeiting legislation was to prohibit the manufacturing of fake Windows holograms. However, the legislation was expanded on July 18, 2002 to provide protection for much of the technology used by DRM. The official summary of the revised legislation states that it would amend “*the Federal criminal code to prohibit trafficking in an illicit authentication feature affixed to or embedded in a phonorecord, a copy of a computer program, a copy of a motion picture or other audiovisual work, or documentation and packaging*”. “*Authentication features*” are defined to be “*any hologram, watermark, certification, symbol, code, image, sequence of number or letters, or other features used by the respective copyright owner to verify that the product is not counterfeit or otherwise infringing of any copyright*”. An “*illicit authentication feature*” is an authentication feature that has been a) “*tampered with or altered*”, b) “*is genuine, but has been distributed*” [...] “*without the authorization of the respective copyright owner*”, or c) “*appears to be genuine, but is not*”.

As in the case of the DMCA and the proposed P2P legislation, a person could be found guilty simply by distributing unauthorized, but not necessarily infringing, copyrighted material. Activities that Congress might want to encourage, such as distance learning and inter-library lending, could be found illegal. If the copyrighted document being distributed were to have undetected authentication features, such as a hologram, those involved with the distribution would not even realize that they had to seek permission to distribute a copy.

Several companies are developing technologies to make computers more secure⁹⁷¹. These technologies are likely to use hardware and/or software to control or restrict the code that can run on protected machines. Once such systems exist, anticounterfeiting legislation could criminalize the dissemination of technology developed to allow legally purchased music and books to be played or read on “protected” machines. Quoting Jessica Litman, an intellectual property law professor at Wayne State University:

Say I've got an MP3 collection and I buy a new nifty player from Microsoft that only plays watermarked content, and I forge the watermark to allow my legal MP3 collection to play. It is certainly the case that if I pass that around, I could be trafficking (in violation of the law).⁹⁷²

Finally, because the law does not require unlawful intent, computer security researchers might, as in the case of the DMCA, find themselves inadvertently running afoul of the law.

⁹⁷⁰ See: <http://thomas.loc.gov/cgi-bin/bdquery/z?d107:s.02395>:

⁹⁷¹ e.g., Microsoft's Palladium and the Trusted Computing Platform Alliance (TCPA).

⁹⁷² See: <http://news.com.com/2010-1071-946732.html?tag=politech>.

II.7 Databases: Treaty and Legislation

In 1991 the U.S. Supreme Court ruled in *Feist Publications v. Rural Telephone Service*⁹⁷³ that telephone books are not protected by U.S. copyright law, because the alphabetical arrangement of telephone listings does not satisfy the creativity requirement of copyright. Since that decision, phone companies, Thomson (owner of West Publishing, the publisher of legal decisions), the American Medical Association (publisher of the *Physician Desktop Reference*), and the stock exchanges have joined with other content providers in lobbying for new protection for collections of facts or databases.

Five years after *Feist* the European Union Database Directive⁹⁷⁴, which extends copyright-like protections called “*sui generis*” (Latin for “of its own kind”) to collections of facts, was passed with little to no involvement of the scientific and technical community. The Directive prohibits unauthorized copying of databases for fifteen years; “substantive” changes to a database trigger a new fifteen years of protection. It’s not clear how significant the changes have to be to protect the entire database. However, it is likely that most databases will retain protection throughout the time that they are of commercial value, since they need only be modified enough to restart the clock. EU member states are allowed to provide fair use types of consumer rights, but these potential rights are more limited than traditional fair use rights⁹⁷⁵. Database protection extends only to nationals or residents of an EU member state, though it’s likely that the EU would extend protection to other countries that pass similar legislation.

Shortly after the passage of the EU Directive, the U.S. government proposed a database treaty at the 1996 WIPO meeting. A letter⁹⁷⁶ from the Presidents of the National Academy of Science, the National Academy of Engineering, and the National Institutes of Health, a portion of which is quoted below, played a key role in preventing the passage of the database treaty.

We believe that these changes to the intellectual property law, if enacted in their present form, would seriously undermine the ability of researchers and educators to access and use scientific data, and would have a deleterious long-term impact on our nations research capabilities. Moreover, the proposed changes are broadly antithetical to the principle of full and open exchange of scientific data espoused by the U.S. government and academic science communities, and promoted internationally.

Since the unsuccessful attempt to pass a treaty, there have been several efforts to pass database legislation in the U.S. Congress⁹⁷⁷, including the insertion of a

⁹⁷³ See: <http://floridalawfirm.com/iplaw/feist2.html>.

⁹⁷⁴ See: <http://europa.eu.int/ISPO/infosoc/legreg/docs/969ec.html>.

⁹⁷⁵ for a discussion of fair use limitations and other aspects of the Directive see: <http://www.nfais.org/WhitePapersDetails.asp?PublicationID=16>.

⁹⁷⁶ See: <http://arl.cni.org/info/frn/copy/data.html>.

⁹⁷⁷ For a more detailed discussion see: <http://www.acm.org/usacm/IP/database.htm>.

database provision into a version of the DMCA⁹⁷⁸. The National Research Council also produced a report entitled *Bits of Power*⁹⁷⁹ in which they warned about overly protective database legislation and called for “full and open exchange of scientific data resulting from publicly funded research”.

The last time that database legislation was introduced was in 1999, at which time there were two competing bills, the Collections of Information Antipiracy Act⁹⁸⁰ (Coble R-NC) and the Consumer and Investors Access to Information Act⁹⁸¹ (Bliley R-Va). The Coble bill has many similarities to the DMCA, while the Bliley bill resembles the Campbell/Boucher bill. Both ban the wholesale misappropriation of database, but they differ on how to deal with the creation of new databases using material from existing ones (transformative use). The Coble bill prohibits the use of a “substantial part” of a database in many instances, but allows a limited kind of fair use if the fair use does “not materially harm the primary market for the product or service”. Just how one would determine whether or not the extraction of specific information from a database would impact a market is not defined. By contrast, the Bliley bill allows the access and reuse of information to create new databases, so long as the new databases are not “substantially the same” as the original database.

The Coble bill resembles the EU Database Directive by providing fifteen years of protection for the database, with revised portions getting an additional fifteen years of protection. It’s not obvious how one determines which portions of a revised database retain protection and for how long that protection lasts. This determination is not a problem with the Bliley bill, because it permits transformative uses. Bliley also specifically excludes facts from protection:

Protection for databases [...] does not extend to the sale or distribution to the public of a duplicate of any individual idea, fact, procedure, system, method of operation, concept, principle, or discovery.

Like the DMCA, the Coble bill allows for significant criminal penalties — up to five years in jail and a fine of \$250,000 for the first offense, both of which are doubled for a second or later offense. The Bliley bill, like the Campbell/Boucher bill, has only civil penalties, with convictions being treated as unfair or deceptive acts under the Fair Trade Commission Act. The maximum fine for each penalty is \$10,000.

Since 1999 proposed database bills have been circulated but not introduced in Congress. Because of concerns about the impact that such legislation might have on the scientific enterprise, the Presidents of the three Academies, together with the Association of American Universities, the American Association for the Advancement of Science, the American Council on Education, and the National

⁹⁷⁸ The Presidents of several key scientific and engineering societies sent a letter objecting to the database provision: <http://www.acm.org/usacm/IP/presidents-letter-998.htm>

⁹⁷⁹ See: <http://www.nap.edu/readingroom/books/BitsOfPower/>.

⁹⁸⁰ See: <http://thomas.loc.gov/cgi-bin/query/z?c106:H.R.354.IH.>

⁹⁸¹ See: <http://thomas.loc.gov/cgi-bin/query/z?c106:H.R.1858.IH.>

Association of State Universities and Land-Grant Colleges sent a letter⁹⁸² to Rep. Jim Sensenbrenner, Jr., chairman of the House Judiciary Committee, about possible legislation. The letter stated:

We recognize a need to fill a gap in intellectual property law, one that would protect proprietary databases against parasitical copying and promote public dissemination of databases that might otherwise not be published for fear of misappropriation. At the same time, we have testified to a set of concerns about the deleterious effects that overprotection would have on the nation's research and educational systems due to reduced access to and use of factual information, including the constriction of the constitutionally protected public domain in data. Thus, while we would like to see the adoption of appropriately focused database legislation, we cannot support legislation that, in our judgment, would do more harm than good by unreasonably restricting access to and use of information that does not otherwise meet the standards of originality and creativity under copyright law.

While it's likely that a database bill will eventually become law in the U.S., it remains to be seen if that bill will focus on preventing the wholesale misappropriation of commercial databases or if it will be so broad as to represent a threat to scientific and other intellectual endeavors.

III Court Cases

III.1 Eldred v. Ashcroft — Challenging the Time Extension to Copyright

One might ask how extending copyright to the life of the creator plus almost three quarters of a century encourages creativity. Is this really what the Founding Fathers meant when they used the phrase “limited time”?

Eric Eldred doesn't think so. Eldred runs a website⁹⁸³ that publishes public domain material, some of which received retroactive copyright protection with the passages of the Sony Bono Copyright Term Extension Act (CTEA). When the CTEA was passed, Eldred, together with Laura Bjorklund, who publishes genealogy texts and out of print books, sued to get the extension declared unconstitutional.

Eldred v. Ashcroft was argued before the U.S. Supreme Court by Stanford Law School professor Lawrence Lessig on Oct. 9, 2002, and on January 15, 2003⁹⁸⁴ the Court upheld copyright extension by a 7–2 vote. Amicus briefs in support of Eldred were filed by law professors, economists, library associations, historians, the Project Gutenberg Literary Archive Foundation, the Free Software Foundation, and others. There is also a “creators” brief signed by organizations including the Apache Software Foundation, the National Writers Union, USACM, and

⁹⁸² See: <http://www.aau.edu/intellect/DatabaseLtr1.25.01.html>.

⁹⁸³ See: <http://www.eldritchpress.org/>.

⁹⁸⁴ Legal opinions and briefs can be found at: <http://eldred.cc/news/>.

the Computer and Communications Industry Association. An Intel Corporation brief in partial support states, “Intel submits that for the first time in history the rich promise of the public domain is within the grasp of entire generations of new creators, due to the liberating power that digital computing, networking, and communications technologies deliver to the average citizen. [...] The notion that a *de facto* perpetual copyright term is sanctioned by the Constitution as long as each individual extension is of limited duration seems inherently flawed and unable to withstand scrutiny in light of the balanced need for a rich and vibrant public domain and the plain language of the Copyright Clause itself.”

The idea that creative works should eventually enter the public domain is a key consideration for those who argue that the length of copyright needs to be more limited than it is under the CTEA. Quoting from the Eleventh Circuit Court’s opinion in *The Wind Done Gone*⁹⁸⁵, a parody by Alice Randall of *Gone With the Wind*:

The second goal of the Copyright Clause is to ensure that works enter the public domain after an author’s rights, exclusive, but limited, have expired. Parallel to the patent regime, the limited time period of the copyright serves the dual purpose of ensuring that the work will enter the public domain and ensuring that the author has received “a fair return for [her] labors.” This limited grant “is intended to motivate the creative activity of authors [...] by the provision of a special reward, and to allow the public access to the products of their genius after the limited period of exclusive control has expired.” The public is protected in two ways: the grant of a copyright encourages authors to create new works, [...] and the limitation ensures that the works will eventually enter the public domain, which protects the public’s right of access and use.

III.2 DVD Related Cases

I shall review several cases that relate to DVDs, two based on the DMCA and a third that relies on trade secret law. DVDs have become important in the copyright debate because the digital version of movies are encrypted on DVDs to prevent copying. Before a DVD can be played, the DVD player must determine how to decrypt the DVD by using an appropriate “key”.

It is not necessary to decrypt a DVD in order to make large numbers of illegal copies. In fact, a commercial operation that manufactures illicit DVDs will produce encrypted versions so that they will play on standard DVD players. The ability to produce decrypted versions of DVDs is of no benefit to such unlawful operations.

In order to understand the subtleties of the issues, we first need to examine the copy-protection technology used for DVD and why it was easily broken.

⁹⁸⁵ See: <http://laws.lp.findlaw.com/11th/0112200opnv2.html>.

DVDs are encrypted using a 40-bit⁹⁸⁶ encryption scheme called Content Scrambling System (CSS). A trade organization called the DVD Copy Control Association (DVD CCA) licenses the manufacturers of DVD players and computer systems that play DVDs. In order to be licensed, the licensee must not only pay a fee but also sign a non-disclosure agreement. Since a fundamental principle of open software systems such as Linux and GNU is that all of the software is available for anyone to see, a non-disclosure agreement that requires that CSS be kept secret is inconsistent with open software. Another obstacle for advocates of open or free software is that, unlike a corporate entity such as Microsoft, there typically is no single person who can make a legal commitment that is binding on the software writers.

Legally purchased DVDs can be played on computers running Windows, but they cannot be played without first being decrypted on computers running Linux. Consequently, some Linux users felt that they had an ethical, if not legal, right to break CSS.

Breaking CSS was relatively unchallenging, since CSS is a weak encryption system for several reasons. First, a 40-bit key can be calculated by using exhaustive search over all possible 40-bit strings to find the actual key. Such an exhaustive search can be done in a relatively short period of time on modern computers. Second, while at first glance it would appear that a secret encryption system is more secure than a public or open one, the opposite typically is true, because strong (difficult or impossible to break) encryption is very hard to derive. Therefore, experts generally recommend systems that have been subjected to intensive scrutiny and are widely believed to be secure. Nonetheless, the creators of CSS chose to develop a secret system. They also attempted to strengthen CSS by making it somewhat convoluted (obfuscation). But obfuscation, while not necessarily increasing the difficulty of breaking an encryption system, can increase the difficulty of verifying that the system is secure. Finally, because DVDs have to play on machines produced by different manufacturers and because they have to play even if a key is compromised, each DVD contains a list of keys — one for each “official” manufacturer and some extra keys that can be used in case some of the initial keys are broken. Therefore, in order to decrypt a DVD, you need to know only the location (offset) on the DVD of the key for your machine.

Not surprisingly, CSS was broken relatively quickly. Just who did what is a bit unclear.

III.3 Jon Johansen

On January 24, 2000 Jon Johansen, a 16 year old Norwegian, was accused of having created DeCSS, a scheme for decrypting CSS a few months earlier, when he was still 15. While everyone acknowledges that Johansen posted DeCSS on his website, there is some question as to who actually developed DeCSS. One

⁹⁸⁶ 40-bits refers to the length of the “key” or number that is needed to encode the digital material. The longer the key, the harder it is to decode without additional information.

claim is that CSS was broken by an anonymous German programmer and that a group called Masters of Reverse Engineering (MoRE) wrote the software. If true, then Johansen's only "crime" would have been the posting of DeCSS on his website.

Johansen's home was searched, but he was not actually indicted until January 9, 2002. He was acquitted of all charges in a unanimous decision by an Oslo City court on January 7, 2003. Head Judge Irene Sogn stated, "The court finds that someone who buys a DVD film that has been legally produced has legal access to the film." She also said that Johansen could use whatever techniques he wished to view legally purchased DVDs.

The prosecution in the Johansen case has appealed, and as a result the case will be retried in the summer of 2003. One possible explanation for the prosecutorial action is to keep the Bunner case (see below) alive.

III.4 Universal City Studios, Inc. v. Reimerdes

On Jan 14, 2000 the Motion Picture Association of America (MPAA) filed injunction complaints against several defendants who had posted DeCSS on their websites⁹⁸⁷. All but one of the defendants complied; Eric Corley, publisher of an electronic magazine called *2600*, refused to remove DeCSS from his website. Consequently, he became the lone defendant.

The MPAA accused Corley of violating the anti-circumvention provisions of the DMCA. The defense argued that code is a form of speech and that the posting of DeCSS was covered by fair use and by several exceptions contained in the DMCA. Judge Lewis A. Kaplan of the Southern District of New York was not convinced. On Aug. 17, 2000 Judge Kaplan enjoined *2600* for both posting and linking to DeCSS, stating⁹⁸⁸:

Defendants, on the other hand, are adherents of a movement that believes that information should be available without charge to anyone clever enough to break into the computer systems or data storage media in which it is located. Less radically, they have raised a legitimate concern about the possible impact on traditional fair use of access control measures in the digital era.

Corley appealed Kaplan's decision to the Second Circuit Court of Appeals. Although the case for the defense was argued by Stanford Law School Dean Kathleen Sullivan, the Appeals Court affirmed Judge Kaplan's decision⁹⁸⁹ on Nov. 28, 2001. Many observers were surprised by the affirmation of the anti-linking portion of the decision, since DeCSS is widely available on the Internet⁹⁹⁰.

The case is not being appealed.

⁹⁸⁷ <http://eon.law.harvard.edu/openlaw/DVD/DeCSS/> gives multiple locations on the internet where copies of DeCSS can be found.

⁹⁸⁸ See: <http://eon.law.harvard.edu/openlaw/DVD/NY/opinion.pdf>.

⁹⁸⁹ See: <http://eon.law.harvard.edu/openlaw/DVD/NY/appeals/opinion.html>.

⁹⁹⁰ Dr. David Touretzky of Carnegie Mellon University maintains a very amusing Gallery of CSS Descramblers at <http://www.cs.cmu.edu/~dst/DeCSS/Gallery>.

III.5 DVD CCA v. Bunner

Andrew Bunner is yet another individual who posted DeCSS on his website. Around the time that Eric Corley was first accused of violating the DMCA, Bunner was charged in a court in California of violating trade secret law by posting DeCSS on his website. The claim is that when Johansen reverse engineered CSS, he violated the anti–reverse engineering clause of the shrink–wrap CSS license. Consequently, Johansen's development — and Bunner's subsequent posting — of DeCSS violated trade secret law.

As of this writing, the trial has not yet occurred. A preliminary injunction was issued that required the removal of DeCSS in either source or object code form. This injunction was appealed, and the Court of Appeals reversed the injunction on the grounds that DeCSS in source code is a form of speech⁹⁹¹ and therefore the injunction was a prior restraint of speech, which is unconstitutional. The Appeals court's decision itself has in turn been appealed to the California Supreme Court, which has not yet ruled on the appeal.

The Bunner case is of interest for a couple of reasons. First of all, it is difficult to understand how the reverse engineering of mass–market software by someone who did not sign a non–disclosure agreement can be viewed as a violation of trade secret law. Second, the Bunner case is predicated on Johansen's violation of the law. But Johansen was acquitted. Could the decision by the prosecution to appeal Johansen's acquittal be an attempt to keep the Bunner case viable?

There are two recent DMCA related court cases that are of special interest to computer scientists: Felten et al and Sklyarov.

III.6 Felten et al. v. RIAA et al.

The Felten case began with a contest sponsored by the Secure Digital Music Initiative (SDMI) in the autumn of 2000. The contest involved “breaking” digital watermarks that were used to protect several on–line snippets of music. A \$10,000 dollar prize was to be divided among the winners — after they signed an agreement assigning their intellectual property rights to the SDMI Foundations and “proponents” of the technologies being used in the contest.

Neither Felten nor any of his co–authors signed the agreement. Instead, they succeeded in breaking all the watermarking technologies and submitted a paper containing their results to the 4th International Information Hiding Workshop. Shortly before their paper was to be present, Felten received a letter from the SDMI on Recording Industry Association of America (RIAA) letterhead, signed by Matthew J. Oppenheim, Esq., RIAA's Vice President for Legal Affairs. The anti–dissemination provisions of the DMCA were used to threaten the authors, their employers, the program committee members, and all of their employers⁹⁹². Because of the financial risk to so many individuals, the paper was withdrawn

⁹⁹¹ Contrary to a number of other court rulings, the Appeals court found that DeCSS in object code is not a form of speech.

⁹⁹² See: <http://www.cs.princeton.edu/sip/sdmi/riaaletter.html>.

from the workshop at the last minute. A few hours after the withdrawal, Openheim and the SDMI issued a statement claiming that the SDMI had never intended to bring suit.

The paper was subsequently presented at the USENIX Security Symposium. In April 2001, prior to USENIX presentation, the authors of the USENIX paper — Ed Felten, Bede Liu, Scott Craver and Min Wu, all of whom were at Princeton University at the time, Dan Wallach, Ben Swartzlander, and Adam Stubblefield, all of whom were at Rice University, and Drew Dean, who had been at Xerox PARC — filed suit together with the USENIX Association. The defendants were the RIAA, the SDMI, Verance, Attorney General John Ashcroft, and four “Doe” companies (not known to the plaintiffs).

The issues raised in the Felten case are not limited to a handful of researchers. Professional societies and other publishers of computer science research and development are also at risk. For example, ACM publishes papers in research areas such as watermarks, encryption, authentication, access control systems, tamper resistance, and threat and vulnerability assessment. If any of these articles could be interpreted as dealing with “a technological measure [that] effectively controls access to a work,” ACM could find itself a defendant in a civil or criminal legal case. Consequently, ACM submitted a declaration in support of the plaintiffs⁹⁹³, something that ACM has never done before.

Because the defendants had stated that they had no intention of bringing suit, Judge Garrett Brown of the Federal District Court in Trenton, New Jersey, threw out the case on November 28, 2001 on the grounds that there was no current threat to the plaintiffs.

III.7 U.S. v. ElcomSoft

On July 16, 2001, Dmitry Sklyarov, a Russian computer science graduate student, was arrested at the DefCon Conference in Las Vegas. Sklyarov was accused of trafficking in technology that could be used to circumvent technology protection — in this case the copy protection mechanism for the Adobe eBook. The software that Sklyarov wrote, and about which he spoke at DefCon, was sold by ElcomSoft, the company in Russia at which Sklyarov was employed. ElcomSoft was also indicted under the anti-circumvention section of the DMCA.

Sklyarov’s arrest was triggered by complaints made by Adobe. After his arrest, there was a considerable outcry in the community of software developers, especially since Sklyarov’s activities are not illegal in Russia. Adobe backtracked, but Sklyarov had been arrested by the FBI, which was not about to retreat on the arrest.

Sklyarov was allowed to leave the U.S. on December 13, 2001 after having spent some time in jail followed by time on parole. The Justice Department agreed to withdraw the criminal complaint against Sklyarov, who in turn agreed to return to the U.S. to testify in the upcoming trial.

⁹⁹³ See: http://www.acm.org/usacm/IP/felten_declaration.html.

The scheduled court case was initially delayed until after Dec. 2, 2002, because Sklyarov and ElcomSoft CEO Alex Katalov had been denied visas by U.S. embassy in Russia. When Sklyarov subsequently testified in court, he argued that his only goal was to allow people to make backup copies of eBooks they already owned or to transfer material to a different computer. The jury returned an acquittal on Dec. 17, 2002.

IV Conclusion

Anti-technology copyright legislation threatens the security of our computer based information infrastructure. As a result of legislation such as the DMCA, legislative proposals such as the CBDTPA, and legal cases such as Felten and Sklyarov, computer scientists are engaging in self-censorship. The self-censorship may involve the curtailment of research in some important areas of computer security or the refusal to discuss research with students or colleagues. Another casualty of anti-technology copyright policy is the free and open exchange of scientific information. Non-U.S. researchers are becoming reluctant to present sensitive computer security results in U.S. conferences⁹⁹⁴, publish them in U.S. published journals, and interact with U.S. colleagues.

Digital technology has presented the content industry with an enormous challenge. In response, spokespeople for the content industry are predicting the death of creative activities in the United States as a result of massive piracy, theft, and general lawlessness. Dire warnings about the negative impact on the economy of unauthorized copying have been used to pressure Congress to pass regressive anti-technology legislation that does nothing to address the problem of wholesale illegal copying and sales of copyrighted material by factories operating outside the U.S.

There are countless examples of industries that have been confronted with new technologies that threatened long-standing business models. Either these industries were destroyed because they became obsolete, or they made dramatic changes to their business models and survived. Large content owners, especially Hollywood and the record industry, can survive the threat posed by digital technology to their current business models. But they cannot survive by imposing regressive legislation on the rest of society. They need to develop new business models that provide their customers with the services that they want at a price they think is fair.

If Hollywood and the record industry insist on treating their customers and researchers as if they are all thieves, they will reap what they sow.

⁹⁹⁴ The refusal on the part of some academics both to discuss research with students or to attend U.S. based conferences has already been documented.

Appendix — ACM’s Copyright Policy⁹⁹⁵

ACM has a large and growing digital library that represents a significant investment and source of income. In spite of its obvious interest in protecting its intellectual property, ACM’s copyright policy represents an approach for dealing with copyright that contrasts significantly with the repressive model as represented by the DMCA.

Because ACM policy is developed through volunteer and staff interactions, a lot of thought has gone into how to structure ACM’s copyright policy to balance the needs of the community with those of ACM as a publisher. Here is what ACM’s Interim Copyright Policy says about copying. Note that no permission is required to make copies for personal or classroom use.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, or to redistribute to lists, requires prior specific permission and/or a fee.

ACM’s copyright policy has a section that deals specifically with rights retained by authors.

Rights Retained by Authors and Original Copyright Holders

Under the ACM copyright transfer agreement, the original copyright holder retains:

- *all other proprietary rights to the work such as patent*
- *the right to reuse any portion of the work, without fee, in future works of the author’s own, including books, lectures and presentations in all media, provided that the ACM citation and notice of the ACM copyright are included*
- *the right to revise the work, and*
- *the right to post author–prepared versions of the work covered by ACM copyright in a personal collection on their own Home Page and on a publicly accessible server of their employer. Such posting is limited to noncommercial access and personal use by others, and must include [the ACM copyright notice].*

The employer of an author also is also given some distribution rights:

- *the right of an employer that originally owned copyright to distribute definitive copies of its author–employees work within its organization. Posting these works for world access requires explicit permission from ACM.*

⁹⁹⁵ The ACM copyright policy (Version 4), together with discussions of goals, principles, processes, and how to obtain access to copyrighted works, can be found at: http://www.acm.org/pubs/copyright_policy/.

4.2 Protection of Digital Content and DRM Technologies in the European Union

4.2.1 European Copyright — Yesterday, Today, Tomorrow

*Jörg Reinbothe*⁹⁹⁶

I Introduction

Protecting copyright is an important value that our societies have in common. National legislators introduced the protection of intellectual property more than a century ago, and in some cases even further into the past as an instrument for the distribution of creative works on appropriate terms taking account of the cultural and economic values of creativity. Ever since, the protection of intellectual property has been a history of adaptations to new markets and, in particular, to new technology. The necessary adaptations were usually made on a national basis, by national legislators and national courts. But nowadays, more than ever, national responses to the challenges of technology no longer suffice. As copyright protection has become a truly global issue, it has increasingly had to become structured internationally. This is particularly so at the level of the European Union. The digital environment of the Information Society offers one of the most significant challenges and opportunities for the protection of creativity through copyright and for making copyright “future-proof”, and this includes the application of digital rights management. But we cannot look ahead without bringing back to mind the history of copyright policy in the European Union.

II The Protection of Copyright and Neighbouring Rights

Over the last centuries European countries have played an important role in introducing new intellectual property rights or categories of protection, in adapting copyright to new technologies and new markets and in influencing the making of international law.

It is no exaggeration to say that European countries were among the founding fathers of copyright and neighbouring rights as we know them today. In Europe, legislators have always been particularly aware of the specific nature of copyright protection, which enjoys therefore a long and successful tradition in the Member States of the European Union. All our Member States consider it to be of high value for creativity, investments, job creation, cultural diversity, and, last but not least, for the availability of, and access to, what is nowadays called “content”. Indeed, copyright is an economic, cultural, and societal instrument

⁹⁹⁶ European Commission, DG Internal Market, Head of Unit Copyright and Neighbouring Rights; This presentation reflects the personal views of the author and binds in no way the European Commission or its services.

for fostering creativity, growth, job creation, investments and cultural diversity, and it includes, therefore, economic, cultural, legal and social elements. These elements are the basis for the deal between rightholders and society. Those who are expected to create and invest in creations for the benefit of society at large should receive an incentive and reward in the form of strong intellectual property rights which are balanced against the interests of others and limited in time. The conditions of this deal have to be regularly updated and adapted to market and technology developments. All EU Member States are firmly convinced that this deal is alive and well, just as copyright protection is, and will remain, the useful instrument it was designed to be.

To prove the point about European countries being among the founders of copyright from centuries ago, one could and should mention the Statute of Queen Anne. But more recently it was European countries, which — despite some of them not having a copyright law of their own at that time — structured and adopted the Berne Convention for the Protection of Literary and Artistic Works of 1886, still considered to be the “bible” of international copyright⁹⁹⁷. It was again in European countries that originated intellectual property principles and notions such as moral rights protection, collective management, remuneration systems for private copying, resale rights, copyright contract law or neighbouring rights protection as reflected in the Rome Convention of 1961⁹⁹⁸.

Today, all Member States of the European Union have very detailed and functioning copyright and neighbouring rights legislation. They are all members of the Berne Convention, of the Rome Convention and of the WTO/TRIPs Agreement⁹⁹⁹. Moreover, in the course of 2003, they will all adhere to the so-called WIPO “Internet Treaties”, the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)¹⁰⁰⁰.

III Copyright Legislation in the European Union

III.1 The Copyright Directives of the First Generation

The European Commission realised in the mid 1980s that the Internal Market for free movement of goods and services within the European Union required a legal framework on copyright protection at Community level. Books, newspapers, CDs, films, videos, software or broadcasting — all these products or services are based on material protected by copyright and neighbouring rights. And yet, the concepts of “copyright” or “droit d’auteur” differ among EU Member States, and so does the structure of national copyright laws. The European Court of Justice confirmed in several decisions that harmonisation, legislation at Community level, was called for to safeguard the functioning of the Internal Market in this area¹⁰⁰¹. Since 1988, EU legislation has been prepared. Today, a solid legislative

⁹⁹⁷ See: Berne Convention (1886).

⁹⁹⁸ See: Rome Convention.

⁹⁹⁹ See: TRIPs Agreement (1994).

¹⁰⁰⁰ See: WCT.

framework of seven Directives exists at European Community level in the area of copyright and neighbouring rights, the so-called *acquis communautaire*.

The roots of copyright legislation at European Union level are found in the 1988 Green Paper on “Copyright and the Challenge of Technology”¹⁰⁰². The Green Paper identified six areas where the copyright laws of EU Member States should be harmonised so as to foster the functioning of the European Union Internal Market.

In a first wave, the Green Paper resulted in the adoption of five sector Directives, which harmonised the national copyright laws of the EU Member States. The first generation of such harmonisation concerns the “pre-Information Society age” and was basically enacted between 1991 and 1996. It covers the legal protection of computer programs (1991), rental rights, lending rights and the main neighbouring rights (1992), satellite broadcasting and cable retransmission (1993), the duration of protection of authors’ rights and neighbouring rights (1993), and the legal protection of databases (1996)¹⁰⁰³. The sixth and last initiative of the first generation of copyright harmonisation at Community level is the Directive on the Artists’ Resale Right (the “droit de suite”), and after many years of controversial discussions, Directive 2001/84/EC of 27 September 2001 came into force on 13 October 2001¹⁰⁰⁴.

All these Directives tackle Internal Market needs, are Internal Market instruments and based on Article 95 — the former Article 100 A — of the EC Treaty. It is fair to say that, generally speaking, all these Directives achieve a rather high level of copyright protection and remain faithful to the objectives and the traditions of intellectual property protection in the European Union. At the same time, they reflect a balance between all the rights and interests involved: those of rightholders, commercial users, consumers and the public at large.

Even though these Directives were designed before the arrival of the Information Society with its new services, they are, in fact, already relevant for this new environment. This is true in particular of the Directive on the legal protection

¹⁰⁰¹ Cf. ECJ of 24.1.1989 (“EMI Electrola ./ Patricia”), Case 341/87. ECJ Reports 1989 p. 00079; ECJ of 17.5.1988 (“Warner Bros. ./ Christiansen”). Case 158/86. ECJ Reports 1988 p. 02605.

¹⁰⁰² See: Green Paper (1988).

¹⁰⁰³ See: Council Directive of 14 May 1991 on the legal protection of computer programs (91/250/EEC). OJ L 122/42 of 17.5.91; Council Directive 92/100/EEC of 19.11.1992 on rental right and lending right and on certain rights related to copyright in the field of intellectual property. OJ L 346/61 of 27.11.92; Council Directive 93/83/EEC of 27.9.1993 on the co-ordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission. OJ L 248/15 of 6.10.93; Council Directive 93/98/EEC of 29.10.1993 harmonising the term of protection of copyright and certain related rights. OJ L 290/9 of 24.11.93; Directive 1996/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases. OJ L 77/20 of 27.3.96.

¹⁰⁰⁴ See: Directive 2001/84/EC of the European Parliament and of the Council of 27 September 2001 on the resale right for the benefit of the author of an original work of art. OJ L 272/32 of 13.10.2001.

of databases of 1996. Most, if not all, of the new digital services of the Information Society and of electronic commerce originate in electronic databases, which contain “content”. The Database Directive harmonised at European Union level the copyright protection of databases and introduced the so-called *sui generis* right. One could say that the Database Directive paved the way for the second generation of copyright harmonisation in the European Union.

III.2 Consultations on Copyright in the Information Society

With the advent of the Information Society and the new age of the digital services, so the world has also changed for the protection of intellectual property. Copyright works or subject matter protected by neighbouring rights, such as phonograms, were described as “content”. Service and access providers joined the interest groups, which had always taken an active and lively interest in copyright matters. Those voices, which declared copyright to be an outdated institution soon to be doomed and dumped on the scrap yard of legal history, became louder. Copyright was increasingly considered as an obstacle to the heralded free access to information and “content”, and rightholders were advised to inquire quickly about new forms of economic exploitation of their protected material, notably by way of developing new business models. These new circumstances and the new environment gave an incentive to the *acquis communautaire* at European Union level to be completed with a view to meeting the new challenges of the Information Society also in the area of copyright and neighbouring rights.

With its Green Paper of 1995 on Copyright in the Information Society¹⁰⁰⁵, the European Commission initiated a consultation process, which continued with discussions at several International Copyright Conferences organised by the Commission¹⁰⁰⁶ and the Communication of 1996¹⁰⁰⁷ as a follow-up to the 1995 Green Paper.

IV The Directive on Copyright in the Information Society

The result of these reflections is the Directive on Copyright and Neighbouring Rights in the Information Society, Directive 2001/29/EC¹⁰⁰⁸, sometimes called “the Copyright Directive”. Of course, this title is not accurate, but it stems

¹⁰⁰⁵ See: Green Paper (1995).

¹⁰⁰⁶ “Copyright and Related Rights on the Threshold of the 21st Century”. International Conference. Florence/Italy. June 2 – 4, 1996; “Creativity & Intellectual Property Rights: Evolving Scenarios and Perspectives”. International Conference. Vienna/Austria. July 12 – 14, 1998; “Management and Legitimate Use of Intellectual Property”. International Conference. Strasbourg/France. July 9 – 11, 2000; “European Copyright Revisited”. International Conference. Santiago de Compostela/Spain. June 16 – 18, 2002.

¹⁰⁰⁷ Communication from the Commission: Follow-up to the Green Paper on Copyright and Related Rights in the Information Society. COM (96) 568 final. 20.11.1996.

from the fact that this new Directive is arguably the most important initiative ever adopted at European Union level in the area of copyright. Indeed, it is *the* copyright Directive, it fills gaps in the *acquis communautaire* of the first generation, updates copyright protection by harmonising the right of reproduction and the right of interactive making available of content for all kinds of authors, performing artists, phonogram producers, film producers and broadcasting organisations. It also introduces a Union-wide protection of the so-called technological measures; these new instruments for the digital management of rights. All this amply demonstrates that this Directive truly belongs to a second generation of copyright Directives.

IV.1 Assessment

Some of the highlights of this Directive are worth recalling: Articles 2 and 3 on the rights of reproduction and communication to the public/making available; Article 5 (1) on the exception for technical copies; the concept of “fair compensation” of rightholders for the use of protected works and other subject matter; Article 8 (3) on the claim for injunctive relief against service providers who carry infringing material; and Article 6 on the protection of technological measures, including Article 6 (4), which contains an interface between such protection and certain exceptions to the rights.

The impact and the quality of this Directive should not be underestimated. It lays the ground for the marketing of products and services based on copyright and related rights in the Information Society, and it concerns all groups of rightholders alike. At the same time, it accommodates the legitimate needs of service and access providers as newcomers to the “copyright club”, but equally those of licensees, commercial users and consumers. In short, it is as balanced as can be.

The Directive also harmonises as much as is possible and necessary. Some of those who have criticised the Directive for not achieving enough harmonisation have claimed at the same time that it should have left EC Member States with more flexibility¹⁰⁰⁹. It should not be forgotten, however, that the EU Member States, the European Parliament and the European Commission all clearly endorsed this Directive; the European Parliament with a large majority, and the Council of Ministers with unanimity. The Directive naturally reflects a political compromise. However, the Directive has succeeded in taking account of new technology despite the fact that it is a constantly evolving moving target. It bridges the philosophical gap between “copyright” and “droit d’auteur” countries on the basis of respect for the principle of subsidiarity, which safeguards different legal traditions in the EU Member States. finally, the Directive is based

¹⁰⁰⁸ See: Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. OJ L 167/10 of 22.6.2002.

¹⁰⁰⁹ See: Hugenholtz (2000a); Hart (2002).

on a clear concept, which remains faithful to the previously existing Directives of the *acquis communautaire*.

IV.2 The Implementation of the Directive

The Directive came into force on 22 June 2001. It has to be implemented by EU Member States into their national laws by 22 December 2002. In any event, Member States should implement the Directive as soon as possible and preferably without opening another round of discussions on its provisions. Indeed, there is no time to lose. The adoption and implementation of the Directive is a prerequisite for the ratification by the European Community and its Member States of the so-called “Internet Treaties” WCT and WPPT already mentioned above, which were adopted in 1996 under the auspices of the World Intellectual Property Organisation (WIPO). These Treaties are the basis for treating the “digital agenda” of copyright protection at international level. The European Community has decided, on 16 March 2000, to adhere to these two Treaties together with its Member States¹⁰¹⁰. Moreover, due to the Association Agreements that the European Community has concluded with third countries, more than 20 other countries are to implement the Directive. In those countries, the Directive will serve as a model for the implementation of the obligations under WCT and WPPT. It will, therefore, be the guiding instrument for the ratification of these Treaties by more than 40 countries and the European Community.

As the Directive must be implemented into the national law of EU Member States by 22 December 2002, all Member States have begun drafting their implementing legislation. Regarding the interpretation of the provisions of the Directive, the highest possible degree of common ground must be safeguarded. In order to achieve this objective faithful to the spirit of this legal framework and within the envisaged timeframe, the European Commission has met regularly with Member States, both bilaterally and multilaterally, exchanged views on how to implement the Directive, identified models on how to implement best some of its provisions, and generally offered its assistance. Between May 2001 and October 2002, four multilateral meetings with EU Member States were hosted by the European Commission. On 3 and 4 December 2001, the European Commission organised a two day meeting with Candidate Countries to discuss implementation of the Directive together with other copyright issues of common interest.

V Digital Rights Management

V.1 The Legal Framework

The various meetings of the European Commission with EU Member States have demonstrated that the discussions about implementation of the Directive have

¹⁰¹⁰ Council Decision of 16 March 2000 on the approval, on behalf of the European Community, of the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty (2000/278/EC). OJ L 89/6 of 11.4.2000.

focused on the following issues: limitations and exceptions to the rights, private copying — and the protection of technological measures, in particular digital rights management.

Technological measures, such as copy control or copy management systems, and digitally applied rights management information will form the basis for digital rights management, in short DRM. DRM systems may be applied by rightholders for the marketing of their rights. At the same time, applying such systems constitutes an advantage for all market participants, including consumers, as rightholders may be in a position to offer more protected content on this basis. Protecting these management tools against circumvention and against the production and marketing of circumvention devices is an indispensable condition for the functioning of electronic commerce and for its acceptance among rightholders, commercial users and consumers alike. Moreover, it has been one of the most important parts of the “digital agenda” of copyright since the mid 1990s.

The two WIPO “Internet Treaties” WCT and WPPT of 1996 have demonstrated that the international community of legislators counts on copyright protection and continues to be determined to further adapt it. These Treaties provide for the protection of technological measures and rights management information in Articles 11, 12 WCT and 18, 19 WPPT respectively.

The Directive 2001/29 on Copyright in the Information Society of 22 May 2001 implements the obligations of the 1996 WIPO Treaties WCT and WPPT at European Union level and brings the European Community and its Member States closer to their ratification. As was stated above, the Directive is the precondition and the basis for the ratification.

Article 6 of the Directive implements the respective WIPO Treaty provisions into European Community law with more detail. Not only does it address the protection of technological measures — it contains an entire framework for such protection, including protection against acts of circumvention and so-called preparatory acts; a detailed definition of technological measures; and an explicit interface between the protection and exceptions to the rights, in particular regarding private copying.

It is particularly this interface in Article 6 (4) 1st subparagraph, which is innovative. In a nutshell: being the beneficiary of an exception gives no right to hacking or circumventing technological measures, which prevent such acts. Rather, the beneficiaries of the seven exceptions listed in this provision and the rightholders must co-operate, and only if such co-operation fails, can rightholders be obliged to permit use on an appropriate scale and not to use technological measures to that effect. Only in the case of non-co-operation will the conditions, under which the “locking keys” are handed out, be determined by the Courts or other public authorities. However, these rules do not apply to interactive services, where the conditions for use have been agreed upon by the parties.

This interface between the protection of technological measures and exceptions to the intellectual property rights is structured in a more flexible way with respect

to exceptions for private copying. Under Article 6 (4) 2nd subparagraph, those EU Member States which apply limitations to the exclusive reproduction right for acts of private copying may also oblige rightholders to allow private copying to an appropriate extent without applying technological measures to prevent it. Member States may provide for this obligation, but they do not have to do so. This provision of the Directive takes account of the possible eventual reduction or phasing out of the copyright levies applied at present in most EU Member States. But — and this is crucial — EU Member States will only be ready to abandon or reduce the levies if and to the extent that technological measures are effectively in operation and are accepted by the market, consumers and all parties concerned, and are beneficial and operational also for authors, performers and small corporate rightholders. It could well be imagined, therefore, that the issue of private copying may be the catalyst for the successful introduction of technological measures.

While, therefore, the Directive on copyright in the Information Society forms certainly the most important single element of the legal framework for digital rights management, one shall not lose sight of other elements. The European Commission commissioned a comparative study on conditions applying to copyright licensing contracts under national law. Such licensing conditions, together with the consultation on rights management in the digital environment with particular focus on collective and centralised management, are being fed into the ongoing reflections on the need to supplement the existing legal framework on rights management. The legal aspects of digital rights management were addressed again at the International Copyright Conference entitled “European Copyright Revisited”, which the European Commission organised together with the Spanish Presidency in Santiago de Compostela from 16 to 18 June 2002¹⁰¹¹.

V.2 The Relation between the Legal Framework and Technological Standards

The legal framework of the digital agenda for copyright protection is, as stated above, structured in the Directive on copyright in the Information Society. It is based on a balanced protection of rights and on an equally balanced protection of technological measures. Now technology must breathe life into this legal framework, or, in other words, prevent it from becoming an empty shell. Therefore, while Directive 2001/29 is in the process of implementation by Member States and the reflections on various other aspects of the legal framework on rights management continue, the technical framework has to come into evidence. A valid technical framework can only be based on agreement and it is in the first instance the rightholders who have to be ready to apply it. It would be a mistake to believe that the application of DRM systems could be imposed upon rightholders. However, all other relevant parties must also be involved in order for the technology to be successful. It will only be operational if it is of wide application and if it has been accepted by the market, i.e. by content providers and

¹⁰¹¹ See above Fn. 1006.

commercial users and consumers alike. In addition, the development of divergent or even incompatible standards should nevertheless be avoided.

Establishing a global and interoperable technical infrastructure on rights management in a secure environment appears, therefore, to be a necessary corollary to the legal framework. All governments should try to facilitate such a global infrastructure by offering their good services with respect to research and development and in creating consensus among the (often conflicting) interests of the private sector.

In order to ensure coherence and efficiency, work on the legal framework and on the technical framework and platforms should be linked or proceed in tandem. The challenge of these tasks is considerable; the response is networking between the policy-makers concerned both inside and outside the European Union. Engaging in such networking and search for consensus requires putting the rights and technology into perspective with one another. The desired results are, firstly, to stimulate the creation of and investment in quality content. This cannot be achieved by DRM systems or new business models alone (if seen as alternatives to copyright protection), but through a balanced protection of intellectual property in combination with technological measures. Secondly, legitimate access should be fostered. This calls for prudence concerning the scope of exclusive rights and of technological measures.

VI European Copyright Tomorrow

VI.1 The Fight against Copyright Piracy

Creating a legal framework on substantive copyright law can only be as effective as are the applicable provisions on the enforcement of the rights. Indeed, structuring and harmonising the rules on enforcement of copyright and neighbouring rights at EU level is as important as harmonising substantive law. There is no EU Internal Market of copyright-based goods and services, unless there is solid common ground regarding the rules on enforcement and the approach to fighting piracy. In addition, a solid legal framework at European Union level regarding sanctions and remedies is an indispensable safety net for the functioning of digital rights management in the European Internal Market.

To some extent, certain elements of sanctions and remedies have already been harmonised: the Directive on Electronic Commerce¹⁰¹² harmonised the liability for damages of service and access providers, and the Information Society Directive¹⁰¹³ confirms in its Article 8 (3) the availability of injunctive relief — some may call it “Notice & Take Down” — from those who transmit piracy without necessarily being pirates themselves.

¹⁰¹² Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on electronic commerce). OJ L 178/1 of 17.7.2000.

¹⁰¹³ See above Fn. 1004.

On a more horizontal note, in 1998 the European Commission issued a Green Paper on Combating Counterfeiting and Piracy in the Internal Market¹⁰¹⁴, which was designed to prepare a legislative initiative on enforcement rules. The Green Paper was followed in November 2000 by an Action Plan on the fight against Piracy and Counterfeiting¹⁰¹⁵. This Action Plan announced a series of legislative and practical measures to improve and step up the fight against counterfeiting and piracy in the European Community.

As part of these measures, the Commission is preparing a proposal for a Directive harmonising the legislation of Member States with a view to strengthening the means of enforcing intellectual and industrial property rights. This first horizontal Directive on enforcement will cover the enforcement of both industrial property and copyright and related rights. It is based on the rules already in place in EU Member States and draws upon the WTO/TRIPs Agreement, notably its Part III, which provides for international rules on the enforcement of intellectual property rights. The prepared Directive combines several “TRIPs plus” elements with provisions that reflect best practice in EU Member States. In a second phase, the Commission will examine setting up mechanisms for administrative co-operation among EU Member States. If counterfeiting and piracy are to be fought more efficiently, it appears essential to better co-ordinate the enforcement mechanisms, which already exist in EU Member States. In the medium term, the need to put forward proposals harmonising the minimum thresholds of sanctions and criminal proceedings should also be looked at.

VI.2 The Management of Rights

Intellectual property rights, this cannot be stressed often enough, are significant merchandise. Besides the rules on substantive copyright law and enforcement, the management and licensing of intellectual property rights, both individual and collective, have to be operational for the Internal Market to function properly. Rights management can rightly be called the “third pillar” of copyright protection. An operational management of rights is of particular importance in the context of the new services of the Information Society and is not only of interest for rightholders but also for commercial users, licensees and consumers.

Nevertheless, this issue of rights management, or trading in rights, has so far not been tackled at European Union level and was consequently included in the consultation process initiated by the 1995 Green Paper on Copyright in the Information Society. The consultations revealed indications for the need to harmonise some features of collective management at EC level, as the Commission explained in its 1996 Communication on the follow-up to the Green Paper. Discussions continued, and in November 2000, the Commission organised a two-day hearing on collective management.

¹⁰¹⁴ See: Green Paper (1998).

¹⁰¹⁵ Communication from the Commission to the Council, the European Parliament and the Economic and Social Committee: Follow-up to the Green Paper on combatting counterfeiting and piracy in the single market. COM (2000) 789 final. 30.11.2000.

In the light of this hearing and of numerous written submissions, the Commission is now finalising its conclusions. It appears that the issue of rights management consists of three sub-issues, individual rights management, collective or central rights management and digital rights management. Individual rights management or copyright licensing has very recently been the subject of new legislation in some EU Member States. Collective and central rights management is one of the cornerstones of the Information Society and has been among the most important issues in the context of the consultation of interested circles by the European Commission. Finally, the issue of digital rights management is closely linked to the discussions about the implementation of the Copyright Directive and the application of technological measures.

All these three rights management sub-issues have a pronounced interface with Internal Market rules and the discussions about the creation of so-called “one-stop-shops”, as well as with the application of competition rules to intellectual property. The European Commission will address all rights management issues, together with the interfaces just mentioned, in a Communication on Rights Management in the Internal Market, which will be presented by the Commission in the course of 2003.

VI.3 Updating/Consolidating the *Acquis Communautaire*

Between 1991 and 2001, seven harmonisation Directives were put in place in the area of copyright. At least with respect to the five Directives of the “first generation” — those adopted between 1991 and 1996¹⁰¹⁶ — time seems ripe to identify possible gaps in this harmonisation framework and to put these Directives into perspective with one another, particularly as regards the Information Society Directive 2001/29/EC adopted in 2001. Once identified, such gaps, shortcomings or inconsistencies between the various Directives may lead to a legislative instrument at the level of the European Union, which would update and/or consolidate the legislative framework.

The search for such gaps began already at the European Commission’s International Copyright Conference in mid June this year called “European Copyright Revisited” in Santiago de Compostela¹⁰¹⁷. Other milestones are the Report on the implementation of the Satellite and Cable Directive (adopted by the Commission on 26 July 2002¹⁰¹⁸), the Report on Public Lending Right in the European Community (adopted by the Commission on 12.9.2002¹⁰¹⁹) and the Report on Authorship of Cinematographic Works (adopted by the Commission on 6 December 2002¹⁰²⁰).

¹⁰¹⁶ See above Fn. 1003.

¹⁰¹⁷ See above Fn. 1006.

¹⁰¹⁸ Report from the European Commission on the Application of Council Directive 93/83/EEC on the Coordination of Certain Rules Concerning Copyright and Rights Related to Copyright Applicable to Satellite Broadcasting and Cable Retransmission. COM (2002) 430 final. 26.7.2002.

¹⁰¹⁹ Report from the Commission to the Council, the European Parliament and the Economic and Social Committee on the Public Lending Right in the European Union. COM (2002) 502 final. 12.9.2002.

In November, the Commission's services consulted the High Level Copyright Expert Group on the issue, and in early 2003 it should be on the agenda of the first meeting of the Copyright Contact Committee. Subsequently, the Commission intends to present a Communication on updating and consolidating the *acquis communautaire* on copyright around the last quarter of 2003.

VI.4 Orientations for the Future

While all three essential elements of the legal framework for copyright in the European Union are under active consideration, reflections on the future of EU copyright legislation have entered into a more concrete phase. Sooner or later a response will have to be found for the question as to how much copyright legislation at European Union level is necessary and to what extent national legislation may or should continue to play a separate role. What are the options?

One option would be to further complete the framework of harmonisation of substantive copyright law, where necessary, and add a legal framework on the two other pillars of intellectual property, namely enforcement and rights management including licensing and collective management. This conceptual or sector approach has been followed so far and continues to be the main guiding principle for the European Commission's services responsible for structuring copyright in the Internal Market. Once the three pillars of intellectual property would have been sufficiently harmonised in the European Union, copyright would continue to be granted by the national legislation of EU Member States. The continued application of the principle of territoriality and the (few) remaining differences in national legislation, which are based on legal traditions and have no or limited cross border impact, would cause no obstacles for the functioning of the European Internal Market nor distortions of competition.

Another option is the creation of a European Union copyright code, for instance by way of a Regulation. Under this option, copyright protection would be granted directly at European Union level and apply to its entire territory. It would be a consequent and logical step considering the European Union's economic and legal ties are continuously getting closer. This third option is a call often heard in academic circles — much less, though, among politicians.

Somewhat more realistic, and certainly more popular among politicians, seems to be a third option, which could be described as follows: after the adoption of seven copyright Directives between 1991 and 2001, there is no need for further harmonisation. Under this approach, even harmonising enforcement could be obsolete. Instead of through further harmonisation, the European Internal Market for copyright would, under this option, be finally achieved through the application of the country of origin principle and the mutual recognition of national copyright rules among EU Member States. In fact, these are the classic Internal

¹⁰²⁰ Report from the Commission to the Council, the European Parliament and the Economic and Social Committee on the question of authorship of cinematographic or audiovisual works in the Community. COM (2002) 691 final. 6.12.2002.

Market principles¹⁰²¹. They already apply to areas other than intellectual and industrial property under the Electronic Commerce Directive¹⁰²². In addition, competition law would, on a case-by-case basis, provide for an efficient control of abuse. The decision on the “IMS Health” case¹⁰²³, which is at present pending before the European Court of Justice, may give some indications on the applicable criteria. This third option is, in sum, a combination of the existing harmonisation framework with the application of traditional concepts from the EU Internal Market and EU competition law.

VII Conclusions

Copyright protection was established as an important cultural and economic instrument more than a century ago and in some cases further in the past. National legislation has adapted it continuously to new developments in the markets and technology. More recently, the European Union has undertaken such adaptations with a view to making copyright protection future-proof in the global environment. Despite all the differences in legal and cultural traditions in EU Member States, the European Union has responded to the challenges of the digital environment of the Information Society including Digital Rights Management.

And yet there is no genuine “European Copyright” in place. In the European Union, copyright protection continues to be granted by the national legislation of its Member States who established intellectual property protection. However, seven EU Directives were adopted between 1991 and 2001 in the area of copyright and neighbouring rights. They constitute a solid legal framework and provide for considerable common ground on substantive copyright laws in the European Union. Other initiatives will follow which will provide for a similar degree of common ground regarding the second and third pillars of copyright in the European Union. Indeed, the last two years, in particular, have already laid the ground for the work on the three main issues of the immediate future: enforcement of rights; rights management and updating/consolidating the existing legislative framework at European Union level. Moreover, sooner or later, the question about the (long term) future structure of EU copyright will be answered.

¹⁰²¹ Cf. Report of Lucas, “Pays d’origine contre territorialité” (to be published as part of the Proceedings of the International Conference of Santiago de Compostela (above Fn. 1006).

¹⁰²² See above Fn. 1012.

¹⁰²³ Cf. Decision of the European Commission of 3.7.2001 (COMP D3/38.044 — NDC Health./IMS Health); OJ L 59/18 of 28.2.2002; IMS Health Inc. vs. Commission of the European Communities of 6.8.2001 (Case T-184/01); OJ C 303/19 of 27.10.2001; Decision of the ECJ of first Instance of 26.10.2001 (Case T-184/01 R, IMS Health vs. Commission of the European Communities); OJ C 144/45 of 15.6.2002; Decision on submission for preliminary ruling of LG Frankfurt/M of 12.7.2001 (Case C-418/01, IMS Health GmbH & Co. OHG vs. NDC Health GmbH & Co. KG); OJ C 3/16 of 5.1.2002.

4.2.2 Digital Rights Management and Privacy — Legal Aspects in the European Union¹⁰²⁴

Lee A. Bygrave¹⁰²⁵

I Introduction

As legal phenomena, intellectual property rights and privacy rights have tended to live separate lives. At the same time, regimes for protecting intellectual property have had, up until lately, only a marginal practical impact on the privacy of information users. However, recent developments in Digital Rights Management Systems (DRMS) are bringing to the fore considerable tension between the enforcement of intellectual property rights and the maintenance of consumer privacy. This tension arises not so much out of differences between the basic nature of intellectual property and that of privacy. Rather, it arises from a push by the holders of intellectual property rights (and their intermediaries) to secure their interests by utilising DRMS with the potential to facilitate an unprecedented degree of surveillance of consumers' reading, listening, viewing and browsing habits. The basic purpose of this chapter is to explore this tension and discuss how it is likely to be resolved in terms of European Community (EC) law.

II The Traditional Relationship between Intellectual Property Rights and Privacy Rights

Intellectual property rights and privacy rights share a great deal in their respective origins and agenda. Both have grown to a considerable extent from the same soil provided by doctrines on personality rights. This growth process has involved some cross-fertilisation of the two sets of interests: notions of intellectual property have helped to develop privacy rights, and notions of privacy have helped to develop intellectual property rights.¹⁰²⁶

This cross-fertilisation has existed not just at a theoretical level but also in practice. For example, copyright law has furthered privacy interests by restricting publication of certain film material in which persons are portrayed,¹⁰²⁷ and by restricting the ability of third parties to duplicate and further exploit

¹⁰²⁴ Much of this chapter is based on work published in Bygrave (2002a) and Bygrave, Koelman (2000). Thanks to Kamiel Koelman and Graham Greenleaf for helpful commentary along the way. All following references to Internet addresses were current as of 1st March 2003.

¹⁰²⁵ Norwegian Research Centre for Computers and Law, University of Oslo.

¹⁰²⁶ See, e.g.: Warren, Brandeis (1890): 198 (arguing, *inter alia*, that common law protection of intellectual property is based upon a broader principle of protection of privacy and personality).

¹⁰²⁷ See, e.g., the United Kingdom's Copyright, Designs and Patents Act 1988 (as amended), s. 85(1); Norway's Intellectual Property Act 1961 (*lov om opphavsrett til åndsverk m.v. 12. mai 1961 nr. 2*; as amended), § 45c. For further discussion, see: Theedar (1999).

personal data compiled in certain registers.¹⁰²⁸ Moreover, the exemptions to copyright provided in relation to the “private” or “fair” use of copyright works help to prevent copyright impinging unduly upon the private sphere of information consumers.¹⁰²⁹ At the same time, privacy rights in the form of data protection law aid copyright by limiting the registration and dissemination of personal data that might subsequently be used in breach of copyright.

Nevertheless, there exist fundamental differences between the respective concerns of these two sets of rights. Put somewhat simplistically, the steering axiom for privacy advocates is “knowledge is power”. For holders of intellectual property rights (and their intermediaries), a steering axiom of greater importance is “knowledge is wealth”. More specifically, copyright — broadly conceived — is an attempt to protect the incentive to produce original works and contribute to public well-being by assuring the creators an economic benefit of their creative activity.¹⁰³⁰ By contrast, privacy rights in the form of data protection law attempt to maintain the incentive to participate in a democratic, pluralist society by securing the privacy, autonomy and integrity of individuals.¹⁰³¹

It is also apparent that active consideration by privacy advocates for intellectual property rights has tended to be incidental and *ad hoc*. The concern of copyright-holders for privacy rights can be characterised the same way. Concomitantly, the “private use” and “fair use” exemptions in copyright law are arguably grounded not so much upon privacy considerations but on the interest of the wider community in gaining access to the fruits of creative endeavour.¹⁰³² Indeed, the fact that intellectual property regimes have tended, up until lately, to have had only a marginal practical impact on the privacy of information users is due mainly to two interlinked factors that have little to do with intellectual property law *per se*. First, the sale of copyright material from copyright-holders or their intermediaries to end-users of the material has traditionally been able to be carried out

¹⁰²⁸ See, e.g., the decision of the Federal Court of Australia in *Telstra Corporation Limited v. Desktop Marketing Systems Pty Ltd* [2001] FCA 612, 25th May 2001 in which Telstra Corporation Limited was found to hold copyright in the white and yellow page databases which it publishes. The case caused the shutdown of a reverse phone directory service (“blackpages”) operated by a third party. The service covered major cities in Australia. Given a phone number, it was able to find the name and address of the owner.

¹⁰²⁹ See: Bygrave, Koelman (2000): 99ff.

¹⁰³⁰ See: Sterling (1998): 57–61.

¹⁰³¹ See: Bygrave (2002b): Chapter VII and references cited therein.

¹⁰³² Note, though, that privacy considerations have figured in certain decisions of the German Federal Supreme Court (*Bundesgerichtshof*) limiting the ability of copyright-holders to monitor and prohibit private/domestic audio-recording practices. In this regard, see *Personalausweise* decision of 25th May 1964 [1965] GRUR 104; *Kopierläden* decision of 9th June 1983 [1984] GRUR 54. Similarly, privacy considerations have played a significant role in Norwegian policy here: see, e.g.: *Norges Offentlige Utredninger*, 1983, no. 35, p. 36. For other examples where such considerations appear to have played some role in setting boundaries for copyright, see: Bygrave, Koelman (2000): 102–103 and references cited therein.

as an anonymous cash transaction. Secondly, the material itself has been unable to monitor and report on its usage.¹⁰³³

III Defining Privacy and Related Interests

What is exactly meant by the concept of “privacy”? The concept is notoriously difficult to define precisely, and the considerable literature on the subject proffers a large number of partly conflicting definitions.¹⁰³⁴ For present purposes, “privacy” denotes a state of limited accessibility. More specifically, it denotes a state in which a person (or organisation) is more or less inaccessible to others, either on the spatial, psychological or informational plane.¹⁰³⁵

Privacy as thus defined is closely related to, though not fully commensurate with, autonomy (i.e., self-determination). The latter is an example of an interest which can promote privacy at the same time as privacy can promote it. Such interests are hereinafter termed “privacy-related interests”.¹⁰³⁶ Other important interests in this category are, at the level of the individual, integrity (i.e., a person’s state of intact, harmonious functionality based on other persons’ respect for him/her) and dignity (i.e., a person’s intrinsic worth). At a societal level, important privacy-related interests are democracy (i.e., active participation of citizens in public government of societal processes) and pluralism (i.e., diversity of opinions and lifestyles, plus diffusion of power such that one single group or organisation does not dominate other groups/organisations).

IV The Operational Parameters of DRMS in a Privacy Perspective

The basic functions of DRMS are envisaged as follows:

- (i) controlling access to copyright works (and possibly other information products);
- (ii) restricting unauthorised reproduction (and possibly other usage) of such works;
- (iii) identifying the works, the relevant right-holders (and possibly the conditions for authorised usage of the works); and
- (iv) protecting the authenticity of the latter identification data.¹⁰³⁷

Facilitating each of these functions are a variety of technologies.¹⁰³⁸ These technologies can involve, *inter alia*, steganography (e.g., “digital watermarks”¹⁰³⁹ for

¹⁰³³ For more detail on these and other relevant factors, see: Greenleaf (2002): 37–38.

¹⁰³⁴ For an overview, see: Inness (1992).

¹⁰³⁵ See also, *inter alia*: Gavison (1980): 428–436; Bok (1982): 10.

¹⁰³⁶ For further analysis of such interests, see, e.g.: Bygrave (2002b): Chapter 7.

¹⁰³⁷ See generally Part 2 of this volume.

¹⁰³⁸ Again, see generally Part 2 of this volume. See also: Greenleaf (2002): 43–46; Marks, Turnbull (2000): 212–213; Koelman, Helberger (2000): 166–169; Bygrave, Koelman (2000): 60–61, 108–110.

dissemination and authentication of identification data), encryption (e.g., for controlling access to information products) and various electronic agents (e.g., “web spiders”¹⁰⁴⁰ for monitoring information usage).

It should be stressed, though, that many DRMS are still at the design stage. Accordingly, some uncertainty exists about their exact *modus operandi* once they are implemented on a wide scale.¹⁰⁴¹ For many systems, the exact functions and inter-relationships of some of the system actors — publishers, media distributors, certification authorities, etc. — have not yet been fully delineated. Uncertainty also surrounds the amount and content of data that these actors will register, the precise nature of the payment mechanisms to be employed, and the degree to which various DRMS will be kept separate from other information systems. From a privacy perspective, important questions include the extent to which DRMS will collect and further process *personal* data (i.e., data which relate to, and enable identification of, an individual person — see further *Scope of data protection law* in section V below), the purposes for which these data will be used and the conditions under which they will be disseminated to external actors.

In light of the above-listed functions and technological mechanisms, it is highly likely that many, if not most, DRMS will register at least some personal data relating to purchasers of copyright works (and possibly other information products).¹⁰⁴² This registration will tend to occur pursuant to contract. The registered data could be stored centrally within the system and/or embedded as (part of) digital watermarks in the works themselves. The works might also be configured to enable ongoing (or periodical) registration of the way in which they are used by the purchaser, transmission of these usage data back to a central monitoring service provider, and/or automatic renewal/modification of usage rights on the basis of online interaction with the provider — i.e., what Greenleaf aptly terms “IP, phone home”.¹⁰⁴³

Systems might also register data relating to persons who merely engage in online browsing (i.e., inspecting or sampling an information product without purchasing a particular right with respect to it). Such registration could automatically occur through the use, for example, of “cookies” mechanisms¹⁰⁴⁴ or “web bugs”¹⁰⁴⁵.

¹⁰³⁹ In brief, a “digital watermark” is digital code which is embedded into text, video or audio files and which typically contains data about the usage rights attached to the files: see further Petitcolas in this volume (page 81).

¹⁰⁴⁰ “Web spider” is the name commonly used for Internet search engines — i.e., software robots that trawl, retrieve and index data stored on the Internet, see further: <http://www.monash.com/spidap4.html>.

¹⁰⁴¹ For examples of existing systems, see generally Part 2 of this volume. See also: European Commission (2002); Gervais (1998).

¹⁰⁴² More accurately, what is being purchased is an on-line disseminated copy (or copies) of, and/or certain usage rights with respect to, such materials.

¹⁰⁴³ See: Greenleaf (2002).

¹⁰⁴⁴ By “cookies” is meant transactional data, in the form of a simple text file, about a browser’s Internet activity which are automatically stored by an Internet server on the browser’s computer, often without the browser’s

Alternatively, it could occur more explicitly through making access to material (that has been otherwise “fenced off” using encryption methods) conditional upon disclosure and registration of browser identity.

An additional category of personal data, which will flow through most points of a DRMS, are the unique numbers (International Standard Work Codes or the like) that identify the creators, authors, editors, etc., of copyright works. In the following, however, attention is directed to purchaser- and browser-related data since the processing of these raises the most significant privacy-related issues.

The privacy of purchasers and browsers will be potentially affected at all stages of the data-processing cycle inherent in a DRMS — from the initial registration of data to their subsequent re-usage — at least insofar as the data are personal (i.e., can be linked to an identifiable purchaser or browser). The collection or further processing of the data will tend to render the data subjects (i.e., the person(s) to whom the data relate) more transparent *vis-à-vis* the system operator(s) and possibly external actors.

The data processing could concurrently impinge on a multiplicity of privacy-related interests. The autonomy of a purchaser or browser will be diminished, for example, if a DRMS facilitates the processing of data about them without their consent or knowledge, or if the processing causes them to behave along lines determined primarily by the system operator(s). Further, their integrity could be detrimentally affected and their dignity affronted if the processing does not conform with their expectations of what is reasonable — which will often be the case with non-consensual or covert data processing.

Tensions between DRMS and privacy-related interests are likely to be particularly sharp in connection with the (re-)use of personal data for secondary purposes (i.e., purposes that differ from the purposes for which the data were first collected). A typical example here is when personal data originally collected in order to ensure enforcement of a particular transaction are subsequently employed for the purposes of cross-selling or other marketing of products *vis-à-vis* the data subjects. Such “re-purposing” of data will be especially unsettling if it occurs without the data subjects’ prior consent or if it falls outside their reasonable expectations. It will also be problematic, not just for the data subjects but also the data user(s), if it involves applying the data for purposes for which the data are not suited.

Privacy and related interests could additionally come under fire when copyright-holders (or their representatives) seek information from third parties about the

knowledge. Cookies mechanisms are primarily aimed at customising an Internet service for the browser’s subsequent use of the service or linked services. For further description of such mechanisms and the issues they pose for privacy, see: Mayer-Schönberger (1998).

¹⁰⁴⁵ By “web bugs” is meant minuscule images, commonly in the form of opaque, 1-by-1 pixel GIFs (graphic files), which are embedded in website pages or electronic mail with the aim of transmitting information to a remote computer when the pages or mail are viewed. Their presence and function are usually invisible to browsers. See further: <http://www.privacyfoundation.org/resources/webbug.asp>.

identity of persons who are purportedly infringing copyright. Disclosure of such information could well involve the “re-purposing” of personal data. The current litigation between the Recording Industry Association of America (RIAA) and Verizon Internet Services provides a case in point. Here Verizon — an Internet Service Provider (ISP) — has been served with a subpoena to disclose the identity of one of its customers who is alleged to have unlawfully downloaded music files in which copyright subsists. The RIAA has knowledge of only the Internet Protocol (IP) address of the customer. Verizon is resisting enforcement of the subpoena partly on privacy grounds, but lost in the first round of litigation.¹⁰⁴⁶

The problems described above are not unique to DRMS; they can arise in the context of many other data-processing systems, both commercial and non-commercial. Nevertheless, by their very nature, DRMS will play a pivotal role in determining the character of surveillance of persons’ reading, listening and viewing habits, particularly in what hitherto has been commonly regarded as the private sphere. Monitoring of these habits could well end up being considerably more extensive than previously. Indeed, it is not difficult to envisage a situation in which DRMS come to form a kind of digital Panopticon that not only diminishes consumers’ privacy but inhibits their expression of non-conformist opinions and preferences.¹⁰⁴⁷ These control dynamics would have disturbing implications for the well-being of pluralist, democratic society.¹⁰⁴⁸ Their effect would be exacerbated in tact with the extent to which each DRMS is linked with other information systems containing personal data about consumers.

The amount and content of consumer data which are registered in a DRMS, along with the ways in which these data are further processed, will be determined by a large range of factors. The focus of this chapter is on legal factors, particularly the limitations set by data protection laws. Yet we must not forget that other types of factors — commercial, technological, organisational — play important roles too. For instance, the business backgrounds of the actors running DRMS will have significant consequences for how much purchaser- or browser-related data are registered and the uses to which the data are subsequently put.

As Greenleaf notes, many DRMS

*“will be run directly by publishing houses with lots of different products to shift and a strong interest in secondary use of identified consumption data, or by booksellers with a similar combination of interests. We will not always be ‘lucky’ enough either to have some central industry-based monitoring body standing between consumers and publishers trying to act as an ‘honest broker’, or to be dealing direct with the author who has only her own product to sell. Which business models succeed will have a significant effect on privacy”.*¹⁰⁴⁹

¹⁰⁴⁶ See: *Recording Industry Association of America v. Verizon Internet Services*, decision of 21st January 2003 by Judge Bates of the US District Court for Columbia.

¹⁰⁴⁷ See: Cohen (1996); Bygrave, Koelman (2000); Greenleaf (2002).

¹⁰⁴⁸ On panopticism and its effects, see: Lyon (1994); Gandy (1993).

¹⁰⁴⁹ See: Greenleaf (2002): 51.

At the same time, though, some DRMS operators could conceivably be willing to minimise registration and usage of purchaser- and browser-related data in order to attract the custom of persons who fear for their privacy in the online world. It is well-established that privacy fears pose a major hindrance to broad consumer take-up of electronic commerce.¹⁰⁵⁰ Hence, there exists a marketplace incentive for DRMS operators to attempt to assuage such fears. While consumer concern for privacy is often fickle and myopic,¹⁰⁵¹ the point remains that promotion of consumer privacy can translate into promotion of commercial interests. And the readiness of people to enter into electronic commerce as consumers (or, perhaps more accurately, as “prosumers”) is likely to depend at least in part upon the extent to which they feel assured that their privacy and related interests will be respected by other marketplace actors.

V The Impact of Data Protection Law on DRMS

V.1 Point of Departure for Analysis

The following analysis canvasses the impact of data protection law on DRMS using the EC Directive on data protection of 1995 (hereinafter also “DPD”)¹⁰⁵² as the principal regulatory point of departure. The aim of the analysis is to give a broad-brush treatment of the main issues at hand.¹⁰⁵³

While not the only international regulatory instrument on data protection, the DPD is, in practical terms, the most influential such instrument for the European Union (EU) as a whole.¹⁰⁵⁴ It goes the furthest in terms of providing prescriptive guidance on data protection across a range of sectors. At the time of writing this Chapter, the DPD has been transposed into national legislation by the vast majority of EU Member States, along with most of the East European countries that are poised to gain membership of the Union. Pursuant to its incorporation into the 1992 Agreement on the European Economic Area (EEA), the DPD has also been implemented by those countries that are not members of the EU but

¹⁰⁵⁰ See, e.g.: Bhatnagar, Misra, Raghav Rao (2000); Samarijiva (1997): 282ff.

¹⁰⁵¹ See, e.g.: Froomkin (2000): 1501ff.

¹⁰⁵² See: Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23rd November 1995, 31 et seq.)

¹⁰⁵³ A more detailed analysis is found in Bygrave, Koelman (2000).

¹⁰⁵⁴ For an overview of the other main international instruments, see: Bygrave (2002b): 30ff. Special mention should be made of the provisions on the right to privacy set down in Art. 8 of the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and in Art. 17 of the 1966 International Covenant on Civil and Political Rights. These provisions provide much of the formal normative basis for data protection instruments like the DPD at the same time as they function as data protection instruments in their own right. However, case law developed pursuant to them so far adds little if anything to the principles found in the DPD and, in some respects, falls short. See: Bygrave (1998).

party to the EEA Agreement (i.e., Norway, Iceland and Liechtenstein). Moreover, the Directive exercises considerable influence over other countries outside the E.U., not least because it prohibits, with some exceptions, the transfer of personal data to these countries if they do not provide “adequate” levels of data protection (DPD, Art. 25(1)).

In practice, though, what will directly impact on DRMS is not the DPD as such but national legislation transposing the Directive. On certain points, some of this legislation varies from the Directive and from the equivalent legislation of other EU Member States. This is because the Directive accords Member States a significant margin for manoeuvre when transposing its requirements. Nevertheless, the Directive does not envisage that such variation will incur conflict with its own rules or the respective legislation of other Member States.¹⁰⁵⁵

It is also important to note that the DPD is not the only EC data protection instrument with the potential to affect DRMS operations. The DPD is supplemented by the 2002 Directive on privacy and electronic communications (hereinafter also “DPEC”).¹⁰⁵⁶ The latter Directive replaces the 1997 Directive on privacy and telecommunications.¹⁰⁵⁷ The DPEC is aimed at extending and “fine-tuning” the principles of the DPD so that they may sensibly apply to the provision of “publicly available electronic communications services” that fall within the scope of Community law (DPEC, Arts. 1–3; see also preamble, recital 4). It is part of a regulatory package aimed primarily at regulating transmission networks and services as opposed to the *content* of communications.¹⁰⁵⁸ Although many DRMS are primarily concerned with managing exploitation of content rather than merely facilitating its transmission, parts of their operations could come within the ambit of the DPEC. This is significant because, as

¹⁰⁵⁵ See: Bygrave (2002b): 34–35 and references cited therein.

¹⁰⁵⁶ See: Directive 2002/58/EC of the European Parliament and of the Council of 12th July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (OJ L 201, 31st July 2002, 37 et seq.). The deadline for national implementation of this Directive is 31st October 2003 (Art. 17(1)).

¹⁰⁵⁷ See: Directive 97/66/EC of the European Parliament and of the Council of 15th December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (OJ L 24, 30th January 1998, 1 et seq.) — repealed as of 31st October 2003.

¹⁰⁵⁸ See: Directive 2002/21/EC of the European Parliament and of the Council of 7th March 2002 on a common regulatory framework for electronic communications networks and services (OJ L 108, 24th April 2002, 33 et seq.), particularly preamble, recital 5. Article 2(c) of this Directive defines “*electronic communications service*” as “*a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but excludes services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks*”. The DPEC (Art. 2) applies this definition as well.

pointed out below, the DPEC tightens some of the apparent laxity of the DPD in important respects.

V.2 Scope of Data Protection Paw

Data protection laws focus specifically on regulating various stages in the processing of personal data in order to safeguard the privacy and related interests of the data subjects. A threshold question when seeking to apply such laws is whether the object of purported regulation concerns *personal* data; generally, the laws do not apply unless the data concerned can be properly classified as personal. In other words, a DRMS may be affected by the laws only insofar as it processes such data.¹⁰⁵⁹

The concept of personal data is usually given a broad and flexible legal definition. The following definition in the DPD is fairly representative:

“any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity” (Art. 2(a)).¹⁰⁶⁰

The focus of the definition on the potential of data to enable identification of a person means that “personal data” may encompass, in theory, a great deal of data with *prima facie* little direct relationship to a particular person. Concomitantly, data may be “personal” even if they allow a person to be identified only in combination with other (auxiliary) data.¹⁰⁶¹

However, certain limitations are to be read into the identifiability criterion. Most importantly, the criterion will not be met under the Directive simply by the existence of a remote and purely theoretical possibility of identification; identification must be possible by the use of methods that are “reasonably likely to be used” in the circumstances (recital 26 in the DPD preamble).¹⁰⁶² Further, data will usually not be personal if they can only be linked to a group of persons as opposed to a single (natural/physical) person.¹⁰⁶³

¹⁰⁵⁹ The ambit of data protection laws tends to be delimited according to several other criteria as well (see: Bygrave (2002b): 31, 50–56) but, with respect to DRMS, these criteria are not nearly as significant as the requirement that data be personal.

¹⁰⁶⁰ Recital 14 in the preamble to the Directive makes clear that this definition encompasses sound and image data on natural persons.

¹⁰⁶¹ See: European Commission (1992): 9.

¹⁰⁶² For detailed discussion of this and other factors relating to identifiability, see: Bygrave (2002b): 41ff.

¹⁰⁶³ The data protection laws of some jurisdictions (e.g., Italy and Switzerland) expressly cover data on organised collective entities such as corporations, partnerships and citizen initiative groups: see: Bygrave (2002b): Chapters 9–10. This notwithstanding, such data are only covered if they can be linked back to one particular entity as opposed to a group of entities. The DPEC also expressly provides some protection for the data protection interests of corporations and other legal persons in their role as “subscribers” to electronic communications services (Art. 1(2)): see: *ibid*: 208.

Nevertheless, the legal threshold for what amounts to personal data is low. Thus, many, if not most, DRMS are likely to involve the processing of such data, particularly on purchasers and browsers. It is not possible, though, to determine in the abstract precisely every type of data in a DRMS which will be regarded as personal. This is particularly the case with e-mail addresses, machine addresses (i.e., IP numbers and domain names) and “clickstream” data linked to these.¹⁰⁶⁴ However, the definition of personal data in the DPD is certainly broad enough to embrace such data. Moreover, the DPEC seems to be built on an assumption that at least some such data may be personal (see especially preamble, recitals 24–25).¹⁰⁶⁵ If there exists, for example, a readily accessible directory listing one particular person against one particular address, the latter — along with clickstream data linked to it — are likely to be personal data.¹⁰⁶⁶ The opposite result will pertain if numerous persons are registered against that address. However, the mere possibility of multiple persons sharing a machine with an address registered in the name of only one person is unlikely to disqualify that machine address from being treated as personal data.¹⁰⁶⁷

The extent to which the DPD and similar legislation may cover processing of e-mail addresses, machine addresses and attached clickstream data is not the only point of uncertainty regarding the ambit of data protection laws in a digital context. A closely related point of uncertainty concerns the extent to which these laws may sensibly apply to the operations of electronic agents — i.e., software applications which, with some degree of autonomy, mobility and learning capacity, execute specific tasks for a computer user or computer system. This issue will be of increasing significance as DRMS are likely to involve more and more use of various types of such agents. The issue is only just beginning to be systematically considered.¹⁰⁶⁸

V.3 Regulation of Data Processing

Responsibility for Compliance

Primary responsibility for observing the rules laid down in data protection laws is placed on those actors that control the means and purposes of the processing of data on other persons. These actors are commonly termed “controllers” or “data controllers”. The DPD defines a “controller” as the “natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data” (Art. 2(d)).

¹⁰⁶⁴ By “clickstream” data is meant information on, *inter alia*, which type of computer, operative system and browser program are used, along with lists of visited websites and keywords typed into search-programs. See: Greenleaf (1996a): 91–92; Kang (1998): 1225ff.

¹⁰⁶⁵ Note that the DPEC adopts the same definition of “personal data” as the DPD (DPEC Art. 2).

¹⁰⁶⁶ See: Greenleaf (1996b): 114–115.

¹⁰⁶⁷ See: Bygrave (2002b): 316–318.

¹⁰⁶⁸ For a preliminary analysis, see: Bygrave (2001).

It is important to note that this definition envisages the possibility of there being more than one controller per data-processing operation (i.e., control can be shared). Secondly, a controller need not be in possession of the personal data concerned.¹⁰⁶⁹ Thirdly, who is controller can change from one data-processing operation to another, even within one information system.¹⁰⁷⁰ Fourthly, what is decisive for determining who is controller is not the formal allocation of control responsibilities as set down in, say, contractual provisions, but the *factual* exercise of control.

A controller is to be distinguished from what the DPD terms a “processor” — i.e., a person or organisation engaged in processing personal data “on behalf of” a data controller (Art. 2(e)). Controllers must ensure, through appropriate contractual or other arrangements, that processors carry out their tasks in accordance with the laws that are enacted pursuant to the DPD (Art. 17(2)–(3); see also Art. 16). Liability for a processor’s non-compliance with these laws is put on the shoulders of the controllers (Art. 23(1)).

Accordingly, for the purposes of DRMS operations, it is most crucial to work out which system operators are controllers as opposed to processors. The result of such classification will obviously vary from one system to another, depending on the internal allocation of responsibilities in each. In the following, it is assumed that each system will be run by at least one operator that functions as a controller with respect to the processing of personal data on purchasers and/or browsers.

Core Data Protection Principles¹⁰⁷¹

The application of data protection law to a DRMS means that the system operator(s) — whether controller(s) or processor(s) — must process personal data according to rules that, in sum, manifest an overarching principle that personal data should be processed both *fairly* and *lawfully* (see especially DPD, Art. 6(1)(a)). This principle is manifest, in turn, in rules giving effect to a multiplicity of other principles. In terms of the DPD, the most important of these principles are the following:

¹⁰⁶⁹ See also: Terwangne, Louveaux (1997): 236.

¹⁰⁷⁰ In the context of an electronic communications network, recital 47 in the preamble to the DPD indicates that the person or organisation providing the transmission services (e.g., an ISP) is normally not to be regarded as the controller of personal data contained in a transmitted message; the controller will instead be the person or organisation “*from whom the message originates*”. However, transmission service providers “*will normally be considered controllers in respect of the processing of the additional personal data necessary for the service*”. Such service providers will have to comply with the rules in the DPEC as well as those of the DPD.

¹⁰⁷¹ By “principle” is primarily meant a normative proposition denoting the pith and basic thrust of a set of legal rules. At the same time, these principles have a regulatory force of their own: many of them are incorporated in the DPD and other regulatory instruments as legally binding rules in their own right or as guiding standards that may be applied (by, e.g., data protection authorities) in case-specific interest-balancing processes.

- (i) fair collection principle — personal data should be collected by fair and lawful means (see especially Art. 6(1)(a));
- (ii) minimality principle — the amount of personal data collected should be limited to what is necessary to achieve the purpose(s) for which the data are collected and further processed (see especially Arts. 6(1)(c), 6(1)(e), 7–8);
- (iii) purpose specification principle — personal data should be gathered for specified and legitimate purposes and not processed in ways that are incompatible with those purposes (Art. 6(1)(b));
- (iv) disclosure limitation principle — disclosure of personal data to third parties should occur only with the consent of the data subject or with legal authority (see, e.g., Art. 7(a));
- (v) data quality principle — personal data should be accurate, complete and relevant in relation to the purposes for which they are processed (see especially Art. 6(1)(d));
- (vi) security principle — security measures should be implemented to protect personal data from unintended or unauthorised disclosure, destruction or modification (Art. 17);
- (vii) principle of data subject participation and control — data subjects should be able to participate in, and exercise a measure of control over, the processing of data on them by others (see, e.g., Arts. 7(a), 8(2)(a), 10–12, 14(b));
- (viii) accountability principle — parties responsible for processing data on other persons should be accountable for complying with the above principles (see especially Art. 23).

Three other principles are worth noting too. Each of them can be seen as an elaboration of the above-listed principles. The first is that persons should be given the opportunity to remain anonymous when entering into transactions with others (see especially DPD, Art. 6(1)(e) and (c), together with Arts. 7–8). The second is that persons should be informed of, and given access to, data on them held by others, and be able to rectify these data if inaccurate or misleading (DPD, Arts. 10–12). The third is that fully automated evaluations of a person's character should not be used to reach decisions that significantly impinge upon the person's interests (DPD, Art. 15). The first of these three principles is implicit in the minimality principle, while the latter two are implicit in the principle of data subject participation and control. And, of course, all three are implicit in the overarching principle of fair and lawful processing.

The scope of the latter principle — particularly the fairness criterion in DPD Art. 6(1)(a) — probably extends beyond what is stipulated in the other provisions of the Directive; were this not the case, the Directive's reference to the criterion would be redundant. At the same time, the full scope of the criterion cannot be defined in the abstract. Yet there can be little doubt that a central element of it is a requirement that data controllers respect and therefore take into account the reasonable expectations of the data subjects. This requirement generates in

turn other requirements not all of which are obviously present in the DPD or other data protection laws.¹⁰⁷²

Basic Conditions for Data Processing

The DPD prohibits the collection and further processing of personal data unless the processing satisfies one or more specified conditions. Article 7 lays down the alternative conditions for the processing of personal data generally. These conditions are, in summary:

- (a) the data subject “unambiguously” consents to the processing;
- (b) the processing is “necessary” for the “performance” or conclusion of a contract with the data subject;
- (c) the processing is “necessary” for compliance with a “legal obligation” on the data controller;
- (d) the processing is “necessary” for protecting the “vital interests” of the data subject;
- (e) the processing is “necessary” for performing a task executed in the “public interest” or in exercise of official authority; or
- (f) the processing is “necessary” for the pursuance of “legitimate interests” that override the conflicting interests of the data subject.

Of these conditions, paras. (a), (b), (c) and (f) are most pertinent to the operation of a DRMS. Regarding para. (a), this must be read in light of Art. 2(h), which defines “the data subject’s consent” as “any freely given specific and informed indication of his wishes, by which the data subject signifies his agreement to personal data relating to him being processed”. From this definition, it appears that consent need not be in writing. However, the express registration of consent on paper or electronic medium will aid in fulfilling the requirement in Art. 7(a) that consent be “unambiguous”.¹⁰⁷³ Arguably, the latter requirement will be met even if consent is not explicit (see below), but the data subject’s actions must leave no doubt that he/she has given consent.

In the context of a DRMS, the simple fact that a purchaser takes the initiative to enter into a transaction with a system operator could be seen as a manifestation of consent to the operator’s registration of at least some data on the purchaser. However, this consent will only extend to the registration practices which the purchaser could reasonably expect or about which the purchaser is notified by the operator. Given the concern of the DPD to ensure that data processing is carried out in a manner that is *fair* to the interests of data subjects, notification of the purchaser will have to be done in such a way as to help ensure such fairness. Thus, notification will arguably need to occur *prior* to the purchase transaction taking place (i.e., during the browsing phase), and it will need to involve *active* steps on the part of the operator (i.e., through the latter creating

¹⁰⁷² For elaboration of some such requirements, see Bygrave (2002b): 58–59, 335–336.

¹⁰⁷³ Cf. recital 17 in the preamble to the DPEC (“Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user’s wishes, including by ticking a box when visiting an Internet website”).

screen-icons that can reasonably be said to catch the attention of potential purchasers).¹⁰⁷⁴ The same considerations apply with respect to browsers.

However, the registration of the fact that a person accesses the server of a DRMS — without the person necessarily going on to browse through the server's various pages — is not justifiable under para. (a) if the person is not given an opportunity to consent to that registration. Hence, if a server operates with a mechanism for automatically creating and setting cookies at the time the server is first accessed, and assuming the cookies constitute personal data (see *Scope of data protection law* in this section above), the mechanism will fall outside the bounds of para. (a). Indeed, in the context of DRMS operations, it is hard to see that such a cookies mechanism will meet any of the other conditions in Art. 7, except possibly those laid down in paras. (b) and (f).

The condition set out in Art. 7(b) will often be met with respect to the processing of purchaser-related data in the context of a DRMS given that there will exist a contract between the purchaser and a system operator. The condition may also be satisfied with respect to the processing of browser-related data insofar as the processing is “in order to take steps at the request of the data subject prior to entering into a contract” (Art. 7(b)). The main point of concern is to determine which data processing is “necessary” in both cases.

The necessity criterion should be read as embracing two overlapping requirements: (1) that the processing corresponds to a pressing social or commercial need; and (2) that the processing is proportionate to the aim of the contract.¹⁰⁷⁵ The stringency of these requirements will vary from case to case in accordance with the kind of data processing involved. In other words, exactly which types of data processing will meet the requirements is a question of fact that cannot be answered conclusively in the abstract. The requirements will be clearly met, though, if the relevant system operator registers only those data as are necessary for enforcing the terms of a contract entered into with a purchaser. Such data would probably include the purchaser's name and address, the name and price of the purchased product, together with the date of purchase. It is also clear that the condition in para. (b) will not be met with respect to a data subject who is purely browsing. The condition will only be relevant once the data subject actively requests the system operator to prepare for an imminent purchase transaction.

Less clear is the extent to which para. (b) can properly be used to justify the monitoring of purchasers' private activities *after* a contract is entered into, with the aim of checking compliance with the contract.¹⁰⁷⁶ There can be little doubt that monitoring in pursuit of such an aim may be linked to the notion of contrac-

¹⁰⁷⁴ See also: Terwangne, Louveaux (1997): 239, 241.

¹⁰⁷⁵ Cf. Art. 6(1)(c) of the Directive (personal data must be “not excessive” in relation to the purposes for which they are processed). The term “necessary” in Art. 8(2) of the ECHR is interpreted along similar lines: see, e.g., *Leander v. Sweden* (1987) *Series A of the Publications of the European Court of Human Rights*, No. 116, para. 58.

¹⁰⁷⁶ Cf. the “IP, phone home” function of DRMS described in section IV above.

tual “performance”, but this does not mean that all such monitoring will fulfil the test of proportionality inherent in the necessity criterion. The monitoring could capture in its net a range of personal data that are not strictly required for compliance purposes.

The condition set down in Art. 7(c) could be relevant insofar as the controller has legal obligations towards other DRMS actors. However, solid grounds exist for narrowly construing the term “legal obligation” such that it does not cover purely contractual obligations. Were the term not construed in this way, para. (c) could be used by data controllers to create at will a legal competence to process personal data simply by writing up a contract (to which the data subject is not party). A narrow reading is also supported by the existence and wording of para. (b).¹⁰⁷⁷

If an appropriate legal obligation is found to exist between DRMS actors, a question of fact will again arise as to what data are necessary to process in order to comply with the obligation. The necessity criterion here will be the same as in relation to para. (b) — along with paras. (d), (e) and (f). It is doubtful that the criterion will be met in the case of registration and further processing of data relating to persons who only browse. Hence, the use of cookies mechanisms to register such data will fall outside the scope of para (c).

The condition laid out in para. (f) is perhaps the most flexible and open-ended of the conditions in Art. 7. The Directive provides little useful guidance on how the various interests in para. (f) are to be balanced. Who, for example, is intended to undertake the interest balancing? Recital 30 in the preamble states that, in balancing the various interests, Member States are to guarantee “effective competition”; Member States may also determine conditions for use of personal data “in the context of the legitimate ordinary business activities of companies and other bodies”, and for disclosure of data to third parties for marketing purposes. Otherwise, the Directive leaves it up to the Member States to determine how the interests are to be balanced.

An interesting issue in relation to para. (f) is the extent to which it may justify the use of cookies mechanisms involving non-consensual registration of the fact that a person has accessed the server of a DRMS. The issue is, of course, only pertinent insofar as the data registered (e.g., the address of the visitor’s machine) can properly be viewed as “personal” pursuant to DPD Art. 2(a). As noted above in *Scope of data protection law*, the Directive on privacy and electronic communications seems to be built on the assumption that cookies may contain personal data (see especially recital 25 in the DPEC preamble). Cookies mechanisms may serve the legitimate interests of DRMS operators (see again recital 25 in the DPEC preamble which notes that cookies can be a “legitimate and useful tool” for facilitating, *inter alia*, the “provision of information society services”). However, it is difficult to see how cookies can be deemed “necessary”

¹⁰⁷⁷ Note that Art. 7(c) in an earlier proposal for the Directive referred to an “obligation imposed by national law or by Community law”. See: European Commission (1992): 17, 72.

for satisfying such interests, though admittedly the propriety of such an assessment all depends on how the interests are defined and on exactly what data are registered. If the interests are defined in terms of achieving “best possible conditions for product marketing”, the use of cookies mechanisms might be seen as necessary, even if those mechanisms only generate relatively coarse-grained data about consumer preferences. Yet even if such mechanisms are found necessary, they may well be “trumped” by the data subjects’ interests in privacy, integrity and autonomy. The strength of these interests will increase in tact with the increase in detail and sensitivity of the data generated by the cookies mechanisms.

It is additionally noteworthy that the DPEC permits the employment of cookies mechanisms only for “legitimate” purposes and on the basis that data subjects be notified of, and given the opportunity to refuse, their usage (Art. 5(3); see also preamble, recital 25). However, actual consent of data subjects is not a necessary condition for applying cookies: “access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose” (preamble, recital 25). At the same time, the DPEC fails to clearly specify *when* data subjects are to be notified of cookie usage.¹⁰⁷⁸ In the interests of privacy, the point of departure should normally be that notification shall occur *before* a cookie is stored on the data subject’s computer. Yet, if what the Directive is most concerned about here is to give data subjects an opportunity to refuse cookie storage — notification being merely a means to that end — it could be strongly argued that notification may occur *after* cookie storage since data subjects themselves can easily remove the cookies pursuant to notification.¹⁰⁷⁹

To sum up so far, the four main processing conditions discussed above should, in combination, enable the registration and further processing of certain types of purchaser-related data by DRMS operators. They may also allow for the registration and further processing of certain types of browser-related data, though to a much lesser extent than in the case of data on purchasers.

Sensitive Data

The stringency of the conditions for data processing is increased in some respects for certain classes of data which are deemed to be especially sensitive (see Art. 8). Such data embrace information on a person’s “*racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and [...] health or sex life*” (Art. 8(1)).¹⁰⁸⁰ Determining which data come within these categories will not always be easy, partly because of the vague way in which the

¹⁰⁷⁸ The same omission occurs with respect to DPD Art. 10 (cf. Art. 11) which requires data controllers to inform data subjects about basic details of their processing operations when the data are collected from the data subjects directly. It has been argued that the information must be provided before or at the time of the data collection, see: Bygrave (2002b): 352.

¹⁰⁷⁹ On deletion of cookies, see, e.g., D. Whalen’s “Unofficial Cookie FAQ”, version 2.6, at: <http://www.cookiecentral.com/faq/#2.2>.

categories are formulated and partly because the determination of sensitivity tends to be coloured by context.

A DRMS might involve the processing of some of the above types of data inasmuch as certain personal preferences of purchasers and/or browsers are registered by a system operator. If, for instance, a purchaser enters into a contractual transaction for the use of an information product concerning a particular religious or sexual theme, and the product is registered against the purchaser's name (or pseudonym or other unique identifier), it could be argued that sensitive data about the purchaser have thereby been processed. Yet it could also be contended that the connection between the product's theme and the purchaser's personality in such a case is too remote: i.e., just because a person buys usage rights with respect to a particular product does not necessarily mean that the product reflects the person's own taste; he/she may simply be sampling or analysing a range of different products. The strength of this contention will depend on several factors, including the nature of the product (e.g., an academic treatise on sadomasochism will tend to say less about the purchaser's personal sexual inclinations than, say, a video-clip depicting sadomasochistic rituals for the purpose of viewer enthrallment) and the nature of the transaction (e.g., a one-off transaction will also tend to say less about the purchaser's personal preferences than a series of transactions involving information products that focus on a similar theme). The same sort of analysis will apply with respect to registration of products in which a particular browser shows interest.

Article 8 of the Directive opens with a prohibition on the processing of the above categories of data, but follows up with a list (in Art. 8(2)) of alternative exemptions to this prohibition. In the context of DRMS operations, the relevant exemptions are found in Art. 8(2)(a) — i.e., processing may occur if the data subject explicitly consents to it (except where national laws override this condition) — and Art. 8(2)(e) — i.e., processing may occur if the data in question “are manifestly made public” by the data subject, or their processing is “necessary for the establishment, exercise or defence of legal claims.”

Regarding the first-mentioned exemption, consent must be “explicit”.¹⁰⁸¹ Hence, the process of requesting and providing consent must occur as a formally separate process to the actual purchase transaction. There must be a specific request by the system operator for permission from the purchaser/browser to process the data in question, followed by a specific reply in the affirmative. Arguably too, there must be some sort of record made of the request and reply, with measures in place to keep the record secure from unauthorised access and modification.

¹⁰⁸⁰ Data on “offences, criminal convictions or security measures” are also afforded extra protection under Art. 8(5), though these are less relevant in the context of DRMS. There is some debate about whether the list of data categories in Art. 8(1) is exhaustive or not. The preferred view is that the list is exhaustive, though the loose way in which the categories are formulated makes it possible to interpret them broadly. See: Bygrave (2002b): 344.

¹⁰⁸¹ Cf. the more lenient criterion of non-ambiguity in Art. 7(a).

As for the second-mentioned exemption in Art. 8(2)(e), one issue concerns the meaning of “manifestly made public”. Given the nature of the data involved, the phrase should arguably be interpreted fairly narrowly as indicating an *obvious and conscious readiness* by the data subject to make the data available to *any* member of the general public. The extent to which this condition will be satisfied in the context of a DRMS will depend on the data subject’s understanding of the operational parameters of the particular system. If the data subject believes that the system operates as a closed system *vis-à-vis* other systems (i.e., that the system operators observe strict rules of confidentiality when handling purchaser-/browser-related data), it is difficult to see the condition being satisfied.¹⁰⁸²

Another issue in relation to Art. 8(2)(e) concerns the meaning of “legal claims”. Again, it is strongly arguable that the phrase is not intended to cover claims arising from purely contractual obligations, for the same reasons as are given above with respect to Art. 7(c). Indeed, the sensitive nature of the data involved is an extra ground for reading the phrase in this way. Nevertheless, it is quite possible that national legislation implementing the Directive will allow for data processing in order for a data controller to defend a legal claim in the form of copyright, as the latter is statutorily anchored. Another issue, though, will be the extent to which such processing is “necessary” (as defined above) for the defence of such a legal claim. Here, the necessity criterion should be interpreted strictly since the data in question are regarded as especially sensitive. Thus, “necessary” should be held as denoting a stringent standard of *indispensability*. For instance, while initial registration of such data might be found indispensable for ensuring that copyright is not breached, it will be incumbent on the data controller concerned to delete or anonymise the data once the relevant interests of the copyright holder can be safeguarded in some other way.

Anonymity and PETs

As a general rule, personal data shall be anonymised once the need for person-identification lapses — i.e., personal data must be “kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed” (DPD, Art. 6(1)(e)). This rule should be read in conjunction with the necessity criterion in Arts. 7–8 and the stipulation in Art. 6(1)(c) that personal data be “not excessive” in relation to the purposes for which they are processed. Read together, these rules arguably embody a general principle requiring, as a point of departure, that data-processing systems allow persons to enter into transactions anonymously unless there are overriding legitimate interests to the contrary. It could also be argued, albeit more tenuously, that the rules require active consid-

¹⁰⁸² It is even difficult to see the condition being satisfied in relation to non-virtual shopping: while the purchase of, say, a book in a non-virtual shop will typically be a public act in the sense that any member of the public can incidentally witness the transaction, the purchaser will rarely intend a record of that transaction to be made available (in non-anonymous format) to any member of the public.

eration to be given to developing *technological* tools for ensuring transactional anonymity or, where anonymity is not legally permitted, for ensuring that persons are able to enter into transactions using pseudonyms.¹⁰⁸³

Such tools typically go under the name of “privacy-enhancing technologies” (or “PET’s”). They consist of technical (and, to some extent, organisational) mechanisms that are developed with the aim of reducing or eliminating the collection and further processing of personal data.¹⁰⁸⁴ The DPD provides little *direct* encouragement of PET usage. The closest it comes to expressly mandating such usage is in Art. 17, along with recital 46 of the preamble, yet these provisions are concerned *prima facie* with security measures (i.e., protecting personal data against accidental or unlawful destruction, loss, modification and disclosure) rather than privacy protection more generally.

By contrast, the DPEC is more direct and active in its encouragement of transactional anonymity and thereby of PET usage to facilitate such anonymity.¹⁰⁸⁵ In particular, it states that “[s]ystems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum [...]” (preamble, recital 30; see also more generally Art. 6). As indicated above, a similar stipulation can probably be read into the DPD.

Purpose Specification

Another set of rules with the potential to significantly affect DRMS are those expressing the principle of purpose specification (sometimes also termed the finality principle). The principle is expressed most directly in DPD Art. 6(1)(b) which requires personal data to be “collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes”. In a DRMS context, this requirement has obvious repercussions for the secondary uses to which system operators will be able to put purchaser-/browser-related data.

The principle in Art. 6(1)(b) is grounded partly in concern for ensuring that data are processed in ways that conform with data subjects’ reasonable expectations. It is additionally grounded in concern for ensuring that data are used for purposes to which they are suited (i.e., a concern for adequate information quality).

From the wording of Art. 6(1)(b), it is apparent that the purposes for which the operator of a DRMS registers data on a purchaser or browser must be defined, documented and announced in advance of registration.¹⁰⁸⁶ The purposes must

¹⁰⁸³ Further on the interrelationship of anonymity and pseudonymity, along with their respective significance for privacy/data protection, see: Rossnagel, Scholz (2000); Clarke (1996).

¹⁰⁸⁴ See, e.g.: Burkert (1997).

¹⁰⁸⁵ German legislation is also explicit on this point: see particularly § 3a of the 1990 Federal Data Protection Act (*Bundesdatenschutzgesetz*), as amended in May 2001. See also §§ 4(4), 4(6) and 6(3) of the 1997 Federal Teleservices Data Protection Act (*Teledienstschutzgesetz*), as amended in December 2001.

¹⁰⁸⁶ See: European Commission (1992): 15.

also be notified to the data subject (see also DPD Arts. 10 and 11). Further, they must be “legitimate”. Arguably, the term “legitimate” denotes a criterion of social acceptability which is broader than that of lawfulness, though it is difficult to determine how much broader.¹⁰⁸⁷ The conditions laid down in Arts. 7–8 (see subsections *Basic conditions for data processing* and *Sensitive data* in section V above) provide some, but not exhaustive, guidance on the ambit of the legitimacy criterion. At the same time, a DRMS operator cannot define the purposes of data processing in the same broad and diffuse terms as are found in Arts. 7–8: use of the adjective “specified” in Art. 6(1)(b) indicates that the purposes need to be delineated more concretely and narrowly.¹⁰⁸⁸ Moreover, the legitimacy criterion arguably requires that the specified purposes have (objectively) more than a marginal connection with the operator’s ordinary field of activity.¹⁰⁸⁹ This notwithstanding, the vast majority of DRMS will probably be able to meet the legitimacy criterion fairly easily. Other criteria, particularly those of necessity (dealt with in the preceding sections) and compatibility (see immediately below) will probably tend to pose greater difficulties for system operators.

In terms of the compatibility criterion, if we accept that one of the underlying concerns of Art. 6(1)(b) is to ensure that data are processed in conformity with data subjects’ reasonable expectations, any secondary purpose should not pass the test of compatibility/non-incompatibility unless the data subject is (objectively) able to read that purpose into the purpose(s) first specified, or the secondary purpose is otherwise within the ambit of the data subject’s reasonable expectations.¹⁰⁹⁰ It is doubtful, for example, that a DRMS operator who/which has specified billing as the primary purpose for collecting purchaser data, would satisfy this test if the data were subsequently used for marketing (either by the operator or by others to which the operator has passed the data). In such a case, the “re-purposing” of the data would most probably require prior consent from the data subject.¹⁰⁹¹

The DPEC appears to embrace a fairly stringent version of the purpose specification principle in the relations between communications service providers and service users/subscribers. Traffic data on users/subscribers may only be used for the purpose of marketing the provider’s own services if the subscriber has consented (Art. 6(3)). Otherwise, such data must be erased or made anonymous when no longer needed for purposes of communication transmission, billing or interconnection payments (Arts. 6(1) and 6(2)).

¹⁰⁸⁷ See: Bygrave (2002b): 338–339.

¹⁰⁸⁸ See: European Commission (1992): 15.

¹⁰⁸⁹ Norway’s Personal Data Act 2000 (*lov om behandling av personopplysninger av 14. april 2000 nr. 31*) seems to adopt a similar line when it stipulates that personal data shall be “*used only for explicitly stated purposes that are objectively justified with respect to the activities of the controller*” (“*bare nyttes til uttrykkelig angitte formål som er saklig begrunnet i den behandlingsansvarliges virksomhet*”: § 11(1)(b)).

¹⁰⁹⁰ See: Bygrave (2002b): 340.

¹⁰⁹¹ See: Bygrave (2002b): 335–341 and case references cited therein.

Other Provisions

The rules canvassed in the above sections are likely to have the greatest impact on the running of DRMS. However, numerous other rules in data protection legislation are also likely to have some effect in shaping DRMS operations. These rules deal specifically with, *inter alia*, fully automated profiling practices (DPD, Art. 15),¹⁰⁹² information access rights (DPD, Arts. 10–12),¹⁰⁹³ and the flow of personal data from EU Member States to countries outside the EU (DPD, Arts. 25–26).¹⁰⁹⁴

Moreover, these and many of the rules canvassed in the above sections may be subjected to derogations. For instance, the DPD gives EU Member States the opportunity of adopting legislative measures that derogate from the provisions in, e.g., Arts. 6(1) and 10–12 if it is necessary to safeguard, *inter alia*, “the prevention, investigation, detection and prosecution of criminal offences [...]” (Art. 13(1)(d)), or “the protection of the [...] rights and freedom of others” (Art. 13(1)(f)). Both exemptions are relevant to DRMS and could be used by copyright holders or their representative organisations as leverage points for pressuring Member States into drafting data protection laws that are more “DRMS-friendly” than, say, Arts. 6(1) and 10–12 would *prima facie* allow.

Another such leverage point could be Art. 9 which requires Member States to derogate from the bulk of the Directive’s provisions, with regard to “processing of personal data carried out solely for . . . the purpose of artistic or literary expression” though only if the derogations are “necessary to reconcile the right to privacy with the rules governing freedom of expression”. Of course, Art. 9 is only relevant for DRMS insofar as the basic rationale of such systems can properly be characterised as the promotion of freedom of artistic or literary expression — a debatable point!

VI The Copyright Directive

As intimated in section II above, the impact of DRMS on privacy and related interests is legally regulated not simply by data protection instruments; intellectual property rules play a considerable role too. The most significant of the latter rules in terms of EC law are those contained in Arts. 6–7 of the Directive on copyright of 2001 (hereinafter also “CD”).¹⁰⁹⁵ These provisions afford support for many of the technologies upon which DRMS are based. Article 6

¹⁰⁹² See: Bygrave (2002b): 319–328.

¹⁰⁹³ See: Bygrave (2002b): 352–354; Bygrave, Koelman (2000): 87–88.

¹⁰⁹⁴ See: Bygrave, Koelman (2000): 89–93.

¹⁰⁹⁵ See: Directive 2001/29/EC of the European Parliament and of the Council of 22nd May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ L 167, 22nd June 2001, 10 et seq.). Articles 6–7 build upon and are intended to implement Arts. 11–12 of the World Intellectual Property Organization (WIPO) Copyright Treaty of 1996 (hereinafter “WCT”). See too the mirroring provisions in Arts. 18–19 of the WIPO Performances and Phonograms Treaty of 1996.

stipulates, in summary, that adequate legal protection shall be provided against the intentional circumvention of any effective “technological measures” for protecting intellectual property.¹⁰⁹⁶ Article 7 stipulates, in summary, that adequate legal protection shall be provided against: (a) the intentional and unauthorised alteration or removal of “electronic rights management information”; and (b) the distribution of copyright works from which such information has been removed or altered, in the knowledge that such distribution breaches copyright or related rights.

Both of these provisions are complex and raise numerous issues of interpretation.¹⁰⁹⁷ The following analysis is concerned only with their potential impact on privacy and related interests. More particularly, it focuses on the extent to which these provisions (and the Directive more generally) permit the circumvention of devices (including “technological measures” as defined in Art. 6) which monitor end-users’ reading, listening, viewing or browsing habits. Expressed alternatively, when (if at all) may an end-user take steps to prevent the operation of such devices? Arriving at an answer here involves addressing two questions:

- (i) does prevention breach Art. 6 or 7?
- (ii) if a breach occurs, is it nevertheless permitted under the DPD (or DPEC)?

The relationship between the CD on the one hand and the DPD and DPEC on the other, is complex and difficult to fully delineate in the abstract. How these instruments shall intersect in practice depends largely on how they are transposed in national laws, and in each case EU Member States are given a fairly broad margin of appreciation when carrying out transposition. Importantly, the CD states that its provisions shall be “without prejudice” to legal provisions in other areas, including “data protection and privacy” (Art. 9). Hence, the provisions of the CD do not necessarily trump those of the DPD or DPEC. Yet, as indicated in section V, the latter instruments will not necessarily permit privacy and related interests to prevail over conflicting interests of DRMS operators.

The Meaning of “Technological Measures”

In terms of the potential impact of CD Art. 6 on privacy and related interests, an important issue is whether the concept of “technological measures” extends to devices that *monitor* usage of copyright works. If such devices are not covered, their disablement will not constitute a breach of Art. 6(1). If such devices are covered, their disablement will, *prima facie*, violate Art. 6(1), though the violation could perhaps be justified pursuant to data protection law.

¹⁰⁹⁶ Note that Art. 6 does not apply to computer software, protection for which is to be derived primarily from Directive 91/250/EEC of 14th May 1991 on the legal protection of computer programs (see CD, preamble, recital 50; cf. recital 60 and Art. 9).

¹⁰⁹⁷ For analysis of some of these issues, see: Koelman (2000); Koelman, Helberger (2000): 169 et seq; Kroon (2000): 250 et seq; Hart (2002): 61–63; Retzer (2002); Huppertz (2002); Fallenböck (2002/2003). For analysis of the equivalent issues under Australian and Hong Kong copyright law, see: Greenleaf (2002): 52 et seq.

The CD itself provides no obvious answer to the issue.¹⁰⁹⁸ However, there can be little doubt that some monitoring devices may be covered in light of the broad definition of “technological measures” — i.e., “*any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject matter, which are not authorised by the rightholder of any copyright [or related rights] [...]*” (Art. 6(3)). Potentially augmenting the breadth of this definition is the apparent lack of a requirement that the measure concerned be inextricably linked with protection of copyright (or a related right).¹⁰⁹⁹ On its face, the definition focuses on the prevention or restriction of acts that a rightholder (as opposed to copyright law) has not authorised.¹¹⁰⁰ The extent of authorisation could vary with the whim of each rightholder. Authorisation could cover more than reproduction and dissemination of copyright works; mere access (on an individualised basis) to such works (or possibly other information products) might also be subject to authorisation. This possibility is clearly brought out in subsequent provisions of Art. 6(3) which, in the course of defining when technological measures are deemed “effective”,¹¹⁰¹ refer to “*application of an access control [...] process*” as one way of achieving control of protected subject-matter.

At the same time, the requirement that a technological measure be concerned with prevention/restriction of unauthorised acts in the *normal* course of its operation, most probably means that monitoring devices which are only incidentally concerned with such protection fail to qualify as technological measures.

¹⁰⁹⁸ The same can be said with respect to WCT Art. 11 upon which CD Art. 6 is based. Cf. § 1201 of the US Copyright Act introduced by the Digital Millennium Copyright Act 1998 (Public Law No. 105–304 (1998), codified at US Code, Title 17, §§ 1201–1205). This permits the disablement of monitoring mechanisms tied to access controls, if several cumulative conditions are met (see § 1201(i)). These conditions are, in summary, that: (1) the access controls, in the normal course of operation, collect or disseminate “*personally identifying information*” about the online activities of a person who seeks access to the protected work; (2) conspicuous notice about this information processing is not given; (3) the data subject is not provided the capability to prevent the information being gathered or disseminated; (4) circumvention of the controls has the sole effect, and is solely for the purpose, of preventing the collection or dissemination; and (5) circumvention does not breach another law. These provisions seem clearly aimed at allowing for the disabling of ordinary cookies-mechanisms and web bugs (if all of the above conditions apply). However, doubts have been raised about their application to other monitoring devices that are more integral to copyright-protective technologies; see: Samuelsen (1999): 553 et seq. The practical utility of the provisions is also questionable given that § 1201(a)(2) and (b)(1) restricts the supply of tools that could disable such access controls.

¹⁰⁹⁹ For further discussion of the extent to which technological measures must be connected with copyright protection, see: Fallenböck (2002/2003): section VII(D); Koelman (2000). For parallel discussion with respect to Australian and Hong Kong law, see Greenleaf (2002): 58 et seq.

¹¹⁰⁰ Cf. WCT Art. 11 which refers to acts “which are not authorized by the authors concerned *or permitted by law*” (emphasis added).

¹¹⁰¹ Article 6 applies only to “effective” technological measures.

One might also query whether devices that *merely* carry out monitoring tasks (albeit with protection of intellectual property as the primary purpose) can properly be viewed as “designed to prevent or restrict” unauthorised acts. Pertinent examples here would be devices for the generation and placement of cookies, web bugs and/or web spiders. On the one hand, it could be argued that monitoring *per se* can have the requisite preventative or restrictive function, particularly in light of the increasingly self-evident control dynamics that are central to panopticism.¹¹⁰² Since monitoring facilitates detection of unauthorised actions, it acts as a deterrent for such behaviour, thereby restricting (inhibiting) the behaviour if not, at least in some instances, preventing (stopping) it outright. Part of the argument is that “restrict” is intended to denote a less stringent form of control than “prevent”; if the former term were not so intended, it would risk being made logically redundant by the latter term. The argument as a whole has much to commend it.

On the other hand, the argument is possibly undermined by the requirement that a technological measure be “effective” — i.e., that the measure “achieves the protection objective” (Art. 6(3)). This objective is formulated as a form of “control”. Hence, the issue here turns partly on how “control” is supposed to be understood. That term is not directly defined in the Directive. On its own, “control” is sufficiently flexible to cover the process of behavioural modification described in the preceding paragraph (i.e., detection → deterrence → inhibition). However, the effectiveness requirement could be read as indicating that the control is intended to be relatively concrete, tangible and certain; concomitantly, that the control has an obvious mechanical immediacy in the sense that it must be circumvented before unauthorised use of the protected subject matter is possible. On this view, the control dynamics of monitoring may be deemed as too nebulous and inconsequential to meet the effectiveness requirement. By way of analogy, a contrast can be drawn between the control effect of mounting a video surveillance camera over the unlocked entrance to a house, and the equivalent effect of placing a padlock on the door (and other possible entry points). In the situation where only a camera is used, a would-be intruder could physically enter the house despite the camera (even though the latter may deter such intrusion); in this sense, the camera is not “effective”. In the other situation, a would-be intruder could not physically enter the house unless he/she picked, cut or otherwise disabled the locking device; in this sense, the device is “effective” and thereby analogous to a technological measure as envisaged under Art. 6.¹¹⁰³ The plausibility of this view is strengthened by the fact that it does not render superfluous use of the term “restrict” alongside the term “prevent”. The former term may denote some sort of impediment to accessing or copying which falls short of completely stopping (i.e., preventing) these processes yet which goes beyond merely discouraging them. An example here would be a device that permits access to some but not all of a particular digital product.

¹¹⁰² See: Lyon (1994); Gandy (1993).

¹¹⁰³ Obviously, the fact that the device could be disabled, would not mean that it fails the effectiveness requirement; Art. 6 is predicated on the very possibility of such devices being disabled or otherwise circumvented.

Much the same line of interpretation has been taken in a recent decision by a single judge of the Federal Court of Australia in a case dealing with the meaning of “technological protection measure” under Australia’s federal Copyright Act 1968 (as amended).¹¹⁰⁴ According to Justice Sackville,

“[t]he definition [of “technological protection measure”] [...] contemplates that but for the operation of the device or product, there would be no technological or perhaps mechanical barrier to a person gaining access to the copyright work, or making copies of the work after access has been gained [...] I do not think the definition is concerned with devices or products that do not, by their operations, prevent or curtail specific acts infringing or facilitating the infringement of copyright [...], but merely have a general deterrent or discouraging effect on those who might be contemplating infringing copyright [...]”.¹¹⁰⁵

The judge went on to consider whether this interpretation renders superfluous the term “inhibit” in the definition of “technological protection measure”. He found that the term should be given a narrow construction such that it does not cover mere deterrence or discouragement but a situation in which the extent of unlawful copying is limited as opposed to prevented completely: “A copy control mechanism, for example, might not prevent all copying that infringes copyright, but might limit the extent of unlawful copying [...] for example by reducing the quality of copies that can be made [...]”.¹¹⁰⁶ The judge noted further that while the relevant legislative history — including work on drafting the CD — is not conclusive of the issues here, it is consistent with his interpretation.¹¹⁰⁷

The decision in the case has been appealed and carries little formal weight for interpretation of Art. 6. Yet it is noteworthy given the paucity of other case law on point and given the fact that it indirectly provides considerable benefits for privacy interests.

¹¹⁰⁴ See: *Kabushiki Kaisha Sony Computer Entertainment et al. v. Eddy Stevens* [2002] FCA 906, decision of 26th July 2002 by Justice Sackville (appealed). Under the Australian legislation, a “technological protection measure” means “a device or product, or a component incorporated into a process, that is designed, in the ordinary course of its operation, to prevent or inhibit the infringement of copyright in a work or other subject matter by either or both of the following means: (a) by ensuring that access to the work or other subject-matter is available solely by use of an access code or process (including decryption, unscrambling or other transformation of the work or other subject-matter) with the authority of the owner or licensee of the copyright; (b) through a copy control mechanism” (s. 10). This definition seems to be basically the same as the equivalent definition in CD Art. 6(3). While it does not operate prima facie with an effectiveness criterion as found in Art. 6, the criterion can probably be read into it: see the judgment of Justice Sackville referred to below; see: Greenleaf (2002): 58. Moreover, there is probably little if any substantial difference between the meaning of “inhibit” (s. 10) and “restrict” (Art. 6(3)).

¹¹⁰⁵ See: paragraph 115 of judgment; see too paragraph 117.

¹¹⁰⁶ See: paragraph 116 of judgment.

¹¹⁰⁷ See: paragraph 117 of judgment.

The Scope of “Rights Management Information”

Turning to CD Art. 7, an important privacy-related issue concerns the scope of “rights management information” (RMI). More specifically, the issue is whether personal data relating to a consumer of copyright work are to be treated as a necessary component of RMI. The issue is important because if such data are not to be treated as a necessary component, alteration or erasure of such data by, e.g., an information consumer cannot fall foul of Art. 7(1). RMI is defined in Art. 7(2) as “information provided by rightholders” including “*information about the terms and conditions of use of the [copyright] work or other subject matter*”.¹¹⁰⁸ Does information about “terms and conditions of use” necessarily include data about the identity of users of copyrighted works? Does it necessarily include personal data relating to how the works are used? On its face, the expression “terms and conditions of use” does not comfortably embrace such data.¹¹⁰⁹ This applies *a fortiori* with respect to data on actual usage. However, given that some information usage licences may be quite user-specific, it is arguable that at least data on user identity may be covered.¹¹¹⁰ A fairly clear indication that also information on actual usage of a work may be covered, is found in recital 57 in the preamble to the Directive. According to recital 57, RMI-systems could “*process personal data about the consumption patterns of protected subject-matter by individuals and allow for tracing of on-line behaviour*”.¹¹¹¹ The logic of recital 57, though, is at odds with the fact that RMI is defined as information “provided by rightholders” as opposed to end-users (Art. 7(2)) — ordinarily, data about “consumption patterns” would be provided by end-users, not rightholders. However, the logical tension between recital 57 and Art. 7(2) dissipates if the expression “provided by” is construed somewhat loosely to denote a process whereby rightholders *facilitate* the collection and further processing of the data concerned, thus providing (albeit indirectly) the data.

It could be queried whether Art. 7(1) captures the alteration or removal of RMI when these are not embedded in the copyright work or other protected subject-matter. With respect to the equivalent provisions in Australian and Hong Kong copyright legislation, Greenleaf argues that RMI will only be protected when it is stored in or with the work concerned; concomitantly, elements of RMI will not be protected once they are separated from a work in order to be transmitted

¹¹⁰⁸ The definition of RMI in WCT Art. 12(2) is similar. Note, though, the point of difference described *infra*, n. 1113.

¹¹⁰⁹ Accordingly, it has been claimed that such data appear not to be covered by the definition of RMI in the WCT; see: Bygrave, Koelman (2000): 115.

¹¹¹⁰ See also: Greenleaf (2002): 67 (in relation to definitions of RMI under Australian and Hong Kong law). Bygrave, Koelman (2000): 115 recognise this possibility too. Cf. § 1202(c) of the US Copyright Act (US Code, Title 17) which defines “*copyright management information*” (the equivalent to RMI) as excluding “*any personally identifying information about a user of a work [...]*”.

¹¹¹¹ Cf. Greenleaf (2002): 67: claiming that the definitions of RMI in both the WCT, Australian and Hong Kong legislation do not encompass information about actual usage as they refer only to “conditions” of use.

back to, say, a DRMS server as part of an ongoing monitoring process (“IP, phone home”).¹¹¹² This argument is based on the fact that the Australian and Hong Kong legislation define RMI in terms of information that is “attached” to a copy of a work.¹¹¹³ However, CD Art. 7(2) does not *prima facie* limit the scope of RMI in this way. Hence, RMI or elements thereof will probably still be protected under Art. 7 even if not embedded in or stored with a work or other protected subject-matter.

If personal data about information users are to be treated as a component of RMI — which seems most likely to be the case — the removal or alteration of such data will breach Art. 7(1) only if performed “without authority”. The requisite authority may probably be derived from legislation, particularly legislation on privacy/data protection.¹¹¹⁴ The question then becomes whether and to what extent alteration or erasure of the data is actually permitted or required pursuant to data protection laws. This is a difficult question: as shown in section V, the answers to it will depend on the outcome of complex, relatively open-ended interest-balancing processes that hinge considerably on an assessment of what information processing is “necessary” in the particular circumstances of the case. It will be recalled that the DPD permits the non-consensual registration and further processing of data on consumers of copyright works if the processing is necessary for the performance of a contract or for the establishment, exercise or defence of legal claims or for realising legitimate interests that outweigh the privacy interests at stake.¹¹¹⁵ If these conditions are construed liberally, information consumers will find it difficult to legitimately remove or alter data about them registered by DRMS operators.

Recital 57 in the preamble to the CD stipulates that “technical” privacy safeguards for such data should be incorporated in accordance with the DPD. Thus, the recital goes some way to encouraging the use of PETs. However, from a privacy perspective, recital 57 is disappointing. It seems to link the use of PETs only to the design and operation of RMI-systems, not also to the design and operation of the technological measures referred to in Art. 6. This is rather incongruous as the ongoing monitoring of information usage is most likely to occur

¹¹¹² See: Greenleaf (2002): 67.

¹¹¹³ For Australia, see Copyright Act 1968, s. 10; for Hong Kong, see Copyright Ordinance 1997, s. 274(3). The latter legislation stipulates as an alternative to the criterion “attached” that the information “appears in connection with the making available of a work or fixed performance to the public”. The definition of RMI in WCT Art. 12(2) also refers only to information which is “attached to a copy of a work or appears in connection with the communication of a work to the public”.

¹¹¹⁴ See: Kroon (2000): 254. Note too CD Art. 9.

¹¹¹⁵ Recall too that more stringent conditions apply for the processing of certain categories of especially sensitive personal data (DPD Art. 8), though exactly which types of data would fall within these categories in a DRMS context is somewhat unclear: see subsection *Sensitive data* in section V.

through the application of these technological measures.¹¹¹⁶ Certainly, data protection rules and measures may still apply in the context of Art. 6 — particularly given Art. 9 — but it would have been preferable for the Directive to encourage more directly the use of PETs in that context too. Further, the recital’s reference to the DPD is problematic because, as noted in subsection *Anonymity and PETs* in section V above, that Directive fails to specifically address, let alone encourage, the use of PETs. The DPD also has very little to say specifically about the desirability of transactional anonymity or even pseudonymity (again, see subsection *Anonymity and PETs* in section V above).

VII Considerations for the Future

A considerable degree of uncertainty afflicts the debate about the implications of DRMS. There is uncertainty about the parameters and *modus operandi* of DRMS; uncertainty about the ambit and application of legal rules with respect to both copyright and data protection; and uncertainty about the impact of market mechanisms. Hence, the debate is necessarily based to a large degree on assumptions about potentialities.

Indeed, current concerns about DRMS might end up being largely unsubstantiated. We might be conjuring up a threatening mountain out of what proves to remain a molehill. Several factors could serve to hinder the large-scale implementation of privacy-invasive DRMS. Such systems might be marginalised by market mechanisms — for example, strong consumer preferences for privacy, combined with competition between copyright-holders and their business partners to satisfy these preferences.¹¹¹⁷ The take-up of privacy-invasive DRMS might also be hindered by difficulties in achieving standardisation and compatibility of technological measures.¹¹¹⁸

These uncertainties notwithstanding, future policy must aim to prevent development of DRMS from riding roughshod over privacy. The health of the “digital age” would be dealt a significant blow were the privacy and related interests of information consumers to be sacrificed through technological fiat or one-eyed lobbying on the part of copyright-holders and their business allies. It is very likely that business interests would suffer too: the recording industry (and, to a lesser extent, software industry) already faces a “crisis of legitimacy” particularly with respect to Internet-savvy youth culture. Respect for intellectual property

¹¹¹⁶ Further, as Dusollier points out, the definition of RMI in Art. 7(2) as information “provided by rightholders”, does not accurately apply to the situation in which information usage is actively monitored; such monitoring will rather occur as an automatic function of a technological measure referred to in Art. 6. See: Dusollier (1999): 296.

¹¹¹⁷ See: Samuelson (1999): 565–566; Hugenholtz (1999): 312 (noting previous instances of the market marginalisation of certain anti-copying devices because of their irritation to consumers).

¹¹¹⁸ There has existed a myriad of competing standards with respect to the structuring and provision of RMI. See: Gervais (1998).

rights will be easier to attain if the holders of those rights are seen to respect the privacy and autonomy of information consumers. Further, as noted in section IV, mass take-up of electronic commerce — which should clearly benefit copyright-holders and their business partners — will probably occur only if potential consumers feel that their privacy is not going to be severely compromised.

We are beginning to see some recognition of these points on the part of copyright-holders. In the USA, for example, the Business Software Alliance, Computer Systems Policy Project and RIAA have recently adopted “Technology and Record Company Policy Principles” which mention the need to develop DRMS that “*do not violate individuals’ legal rights to privacy or similar legally protected interests of individuals*” (principle 5).¹¹¹⁹

How industry embracement of such a principle will be translated into practical measures remains to be seen. It is clear, though, that if the principle is to be given proper effect, there will need to be extensive integration of technological measures for protecting intellectual property rights with PETs. Such integration will have numerous facets. One important facet will involve building mechanisms into DRMS architecture which enhance the transparency of the systems for information consumers. Another important facet will involve building mechanisms into the systems’ architecture which preserve, where possible, consumer anonymity, and which allow for pseudonymity as a fall-back option where anonymity is not feasible for legal or technical reasons.¹¹²⁰ At the same time, it may be useful to draw on the technological-organizational structures of DRMS to develop equivalent systems for privacy management.¹¹²¹

In theory, the chances of achieving integration should be increased by the fact that both DRMS and PETs are based on a similar “logical imperative”, this being control of information. Nevertheless, we should not overlook the fact that the economic interests steering many DRMS will not necessarily coincide with the privacy interests of information consumers. Neither should we forget that a large range of technological-organisational devices exist to enforce intellectual property rights in a digital environment and that some of these are more privacy-invasive than others. We need to encourage the development and application of the least privacy-invasive devices. Such encouragement is actually required already by some laws, particularly the DPEC along with German data protection legislation, and it arguably follows, albeit more indirectly, from the DPD and Art. 8 of the ECHR.

¹¹¹⁹ The principles, adopted 14th January 2003, are set out at: http://www.bsa.org/usa/policyres/7_principles.pdf.

¹¹²⁰ See: Feigenbaum (2002). See also the recommendations in: International Working Group on Data Protection and Telecommunications (2000); Greenleaf (2002): 79–81; Information and Privacy Commissioner of Ontario (2002).

¹¹²¹ For preliminary work along these lines, see: Korba, Kenny (2002). More generally, see: Zittrain (2000).

4.2.3 Private Copying and Levies for Information– and Communication–Technologies and Storage Media in Europe

Constanze Ulmer–Eilfort¹¹²²

Abstract: The different European Copyright Laws all provide for certain exceptions and limitations of copyright in which the right holder cannot prohibit certain uses of their work. Copyright levies are to compensate the right holders for the limitations of copyright.

There are great differences between the levy systems in the European Union varying from no levies (and consequently very narrow exceptions and limitations of copyright) in England to a broad range of different levies on both analogue and digital copying media and equipment in Germany.

Levies are being paid by the manufacturers or distributors of copying media and equipment, they are typically being collected by national collecting societies and distributed in accordance with fixed distribution schemes to right holders and authors.

The EU Directive has failed to harmonize levy systems in the European Union. The EU Directive gives, however, certain guidelines as to the amount of a fair levy payment. Furthermore, the EU Directive gives preference to technological protection measures over levy systems. Therefore, to the extent digital media and equipment are concerned, the application of technological protection measures may lead to a phasing out of levy systems.

I Introduction

“Digital right management systems and technical protection measures do not work! They are easy to break or circumvent, they impose unreasonable burdens on private individuals and they hinder the free flow of information. At the end, only the big entertainment enterprises, rich producers and publishers will benefit from such systems and measures, not, however the poor and suffering author, who has created the copyrighted work and who is left with a small lump sum payment.”

These arguments are being raised by the promoters of levy systems. They further state that *“levy systems always work, they allow the private individual to make copies without having to enter a credit card number and they ensure that the author receives a running participation from the use of his or her work.”*

The following will present (i) an overview over the levies imposed and the equipment for which levies are being paid, (ii) the legal framework for levy systems and (iii) some comments on the justification of levy systems in the digital age. As Germany was the first country to impose levy systems and to date has the broadest range and the highest income of levy payments and also since the author is German and knows the German levy system best, a special focus will be put on the German system.

¹¹²² Baker & McKenzie, Frankfurt.

II The Levy Systems

II.1 Levies Imposed on Equipment and Media

Below is an overview of the levies imposed in the European countries on different types of equipment and media.

	A	B	B U	C Z	D K	F I	F	D	G R	H	I	N L	N	P L	P	E	S	C H
Digital Equipment (e.g. CD-recorder, DVD-player)			X	X			X	X		X	X		X	X	X		X	
Reprography (Copiers)	X	X	X	X				X				X				X	X	
Faxes Scanners	X	X						X									X	
PCs/ Hard discs								X										
Printers								X										
Multi-functional Devices	X	X						X				X				X		
Mobile Telephones																		
Digital Media	X	X	X	X	X	X	X	X	X	X	X	X		X			X	X

Tab. 1. Levies on Equipment and Media in Europe¹¹²³

II.2 Equipment / Media

The following is a selection of levy tariffs imposed on equipment and media in different European countries:

Copiers:

- Austria: €10.03 to €338.36
- Belgium: €3.70 to €1,363.70
- Germany: €38.35 to €613.56
- Netherlands: €0.45 /page
- Spain: €45.07 to €222.37
- Sweden: €135.23 to €222.37

Scanners:

- Austria: €307.62
- Belgium: €1.50 to €74.30
- Germany: €10.23 to €255.65

¹¹²³ See: www.eicta.org/copyrightlevies/resources/europeansituation

Faxes:

Austria:	€5.16 to €20.86
Belgium:	€3.70 to €1,363.70
Germany:	€10.23
Sweden:	€0.022 /page

Video Recorders:

Belgium:	3% of wholesale price
France:	€10.00 to €15.00
Germany:	€9.21 to €18.42
Greece:	6% of wholesale price
Spain:	€6.61

PCs:

Germany:	€50.50 ¹¹²⁴
----------	------------------------

Printers / Plotters:

Germany:	€10.00 to €300.00
----------	-------------------

Digital Media (CD-R/RW):

Austria:	€0.15 /hr
Belgium:	€0.13 /hr
France:	€1.26 /hr
Germany:	€0.0614 /hr
Greece:	6% of wholesale price
Netherlands:	€0.42 /hr
Sweden:	€0.15 /hr

The different rates stated for certain equipments relate to the quality, speed and properties of the copying equipment.

While most countries impose levies on digital media, the amount of the levy varies from 0,06/hr in Germany to 0.42/hr in the Netherlands. The differences are partly due to the fact that in Germany levies are imposed on media and on equipment, while in the Netherlands levies are only imposed on media. In some countries the levy is calculated as a percentage (2% to 10%) of the net sale or wholesale price of the media.

On other equipment only few European countries impose levies. This applies, for example, to CD burners and to scanners. No country yet reports that levies on PCs and hard discs are being collected. A levy on PCs in an amount of 2% of the net sales price had been discussed in Greece, but was finally rejected.

In Germany the collecting society VG Wort has filed test cases claiming levies on PCs and printers¹¹²⁵. Further, it is announced that levies will be imposed on mobile telephones and other digital equipment, which is suited to store third party content.

¹¹²⁴ VG Wort has published a tariff of €30 for reprography, ZPÜ has announced (not yet published) a tariff of €20.50 for recordings. The tariff is disputed between Fujitsu Siemens and VG Wort.

¹¹²⁵ See section IV: *Levies on PCs, Printers and other Digital Equipment.*

No copyright levies are being imposed in the United Kingdom and Ireland (as in the United States and Canada), and it was due to lobbying efforts of representatives from the United Kingdom and Ireland that no European levy system was introduced in the context of the European Copyright Directive on the Harmonisation of certain Aspects of Copyright and related Rights in the Information Society (“EU Directive”)¹¹²⁶. Under competition and free trade aspects, such harmonisation would have been desirable as the different levy systems in the European countries lead to severe price differences between IT equipment sold in levy-free countries and IT equipment sold in high-levy countries and encourage shopping in countries which impose no or very low levies.

In Germany levies are also imposed on equipment which may, in fact, not be primarily used for copying protected works. Under Sections 54 and 54 a of the German Copyright Act it is sufficient that the equipment in question provides the *possibility* of copying protected works. The German legislator intentionally took into account that equipment which would be used only to a small degree for copying or recording of copyright protected materials should also be covered by the levy regime¹¹²⁷. The scope of use is to be reflected in the amount imposed on such equipment.

II.3 Collection and Distribution of Levies

Collecting Societies

In Germany and many other European countries, collecting societies are authorized to set levy tariffs, to collect levies and to distribute levies to authors and right holders¹¹²⁸.

In such countries there exist several, sometimes even competing collecting societies. In Germany, for example, levies for private copying are being imposed, among others, by a central office of several collecting societies, including GEMA, for audio and video copying (Zentralstelle für Private Überspielungsrechte — ZPÜ) and by VG Wort and VG Bild Kunst for reprography.

National collecting societies are organized internationally within CISAC (Confédération Internationale des Sociétés d’Auteurs et Compositeurs), BIEM (Bureau International de Edition Mécanique) and IFRRO (International Federation of Reproduction Rights Organisation). Levies collected in the different countries on behalf of foreign right holders - for example the videotaping in France of a movie originating in the United States - are distributed through such international collecting societies to the respective national organizations of right holders.

¹¹²⁶ See section III: *Levies under the EU Directive*.

¹¹²⁷ See: BGH GRUR 1993, 553 — Readerprinter; Recitals to the German Copyright Act of 1985, BT-Drucks. 10/837, p. 10; GEMA v. Hewlett Packard GmbH, decision of May 4, 2000 of the Arbitration Board, p. 11, 12.

¹¹²⁸ In Germany, the authorization to set tariffs is granted to collecting societies in Section 13 of the German Copyright Administration Act (Gesetz über die Wahrnehmung von Urheberrechten und verwandten Schutzrechten).

The German collecting societies are authorized by the German Patent Office upon application (Section 1 et seq. of the Copyright Administration Act¹¹²⁹). They are subject to statutory obligations and governmental supervision. As the collecting societies by way of their assignment need to monopolize the exercise of copyrights, and owing to their public purpose, they are exempt from the application of German antitrust rules (Sec. 24 of the Copyright Administration Act).

In Germany the collecting societies are empowered to set levy tariffs. They may either set the amount of levies unilaterally by publishing such amount in the Federal Gazette (*Bundesanzeiger*) and/ or they may agree on a levy or a reduction of levies with the industries and users paying levies. If, for example, a manufacturer of copiers considers a levy assessed on its equipment to be unfair, it is entitled to negotiate a different tariff with the competent collecting society¹¹³⁰. However, owing to their monopoly position, the collecting societies are bound by the principle of equal treatment. Therefore, different tariffs for the same equipment can only be granted in justified cases, for example in the case of frame agreements with industry associations which handle the collection of levies on behalf of their members.

Collection of Levies

In Germany the levies are being paid by the manufacturer, importer or distributor of the equipment or media on which levies are being imposed, the manufacturer, importer and distributor being jointly and severally liable under the German Copyright Act (§§ 54, 54 a). Manufacturer is the one who actually manufactures the equipment and media. Importer is the one who imports the equipment and media into Germany for commercial sale or for commercial use. Distributor is anybody selling more than 100 pieces of copying equipment or copying media of more than 6,000 hours playing time within a calendar half year in Germany. The responsibility of the importer and distributor has been adopted in order to facilitate the enforcement of levy claims in cases in which foreign manufacturers refuse to pay levies¹¹³¹.

The collecting society VG Wort in 2001 has collected levies for reprographic private uses in Germany in an amount of €56,381,500¹¹³².

The German legislator intended that the levy should finally be borne by the consumers, the users of the copying equipment and media, assuming that the manufacturers, importers or distributors would pass the levy on to consumers by increasing the selling price of the equipment and media. However, owing to competition constraints, the industry today often may not in a position to add the levy onto the purchase price.

¹¹²⁹ Urheberrechtswahrnehmungsgesetz.

¹¹³⁰ See: Section 11 of the German Copyright Administration Act.

¹¹³¹ See: Schricker (1999): § 54, 15.

¹¹³² See: Annual Report of VG Wort for 2001 (<http://www.vgwort.de>).

Copyright levies also have to be paid for equipment ordered on the internet. Any commercial supplier of copying equipment offering such equipment for sale to German customers qualifies as importer under Sections 54 and 54 a of the German Copyright Act and has to pay copyright levies. The only exempted equipment is equipment which is privately imported into Germany.

One of the criticisms against levy systems is that the collecting societies are not successful in imposing levies on every sale of equipment. While the collecting societies address all major manufactures which are selling copying equipment, some of the smaller manufactures, some importers and most of the internet distribution channels have typically not been paying any levies. Given the tight margins and the price sensitivity of consumers in the market for copying equipment, the fact that levies are not uniformly enforced and that in certain European countries no levies are being imposed, constitutes a significant competitive disadvantage. The competitive disadvantage becomes obvious if one compares the levies to the actual sales prices of such equipment. In case of cheap scanners and printers the levy imposed may account for more than 25% of the sales price.

Distribution

The levies collected are, after deduction of the collecting societies' charges, being distributed based on a standardized distribution scheme. According to Section 7 of the German Copyright Administration Act, distribution schemes shall not be arbitrary and shall further the creation of works of authorship. From the levy income for private copying, German collecting societies report that typically publishers and producers receive 30% and authors receive 70%¹¹³³ and in the case of scientific publications, levies are equally shared between authors and publishers¹¹³⁴. By such means, the collecting societies ensure an ongoing stream of income to authors.

Disputes

In Germany, disputes regarding the payment and the amount of levies assessed and the distribution schedules regarding levies have to first be brought before the Arbitration Board at the German Patent Office¹¹³⁵ at first instance and then to the district and higher German civil courts. In a proceeding regarding the fairness of the levy imposed by the collecting societies, the collecting societies carry the burden of proof. It should, however, be noted that in the past the Arbitration Board has regularly upheld the position of the collecting societies that levies have to be paid, and it has only occasionally reduced the levy. For example, on February 5, 2003, the Arbitration Board has suggested that a levy of EUR 12 instead of EUR 30 should be paid for PCs to VG Wort¹¹³⁶.

¹¹³³ See: www.vgwort.de/verteilungsplan.php

¹¹³⁴ See: www.vgwort.de/wissvplan.php

¹¹³⁵ See: Schiedsstelle beim deutschen Patent- und Markenamt, Sections 14 et seq. of the German Copyright Administration Act.

¹¹³⁶ See section IV: *Levies on PCs, Printers and other Digital Equipment*.

III Legal Framework for Levy Systems

III.1 Exceptions and Limitations of Copyright

All European copyright laws provide for certain exceptions and limitations of copyright, i.e., for cases in which the right holder cannot prohibit the use of his or her work. The exceptions and limitations of copyright are being named statutory copyright licenses as the public is granted a license not by the right holder but by statute.

Typical uses of copyrighted works for which exceptions and limitations apply are

- copying for private use,
- copying by public libraries,
- copying for teaching and scientific research,
- copying and distribution of quotations for purpose of criticism or review,
- copying, distribution and modifications for purposes of parody,
- copying and distribution by the press for information purposes¹¹³⁷.

In compensation for the statutory licenses many copyright laws grant the author a right to receive a compensation by way of a levy system.

III.2 Rationales

There are different rationales behind the exceptions and limitations of copyright and the corresponding levy payment:

One of the rationales is of course the principle of free flow of information. Information which has been published should be accessible for teaching and research purposes. The public should benefit from existing information in order to be able to further promote such information¹¹³⁸.

Another rationale, which is behind the private use exception, is to protect the private sphere and to avoid that certain uses which — owing to the technological development — cannot be prevented are being criminalized. Rather than imposing criminal sanctions on a private individual which videotapes a movie to watch such movie at a different time, many European legislatures have decided to exempt such use from the exclusive rights of copyright, to grant statutory licenses for such specific uses and to compensate the right holders by way of the levy system¹¹³⁹.

Last but not least, in Germany levies compensating exceptions and limitations of copyright are a means to outbalance a disparity of negotiation powers between right holders and authors and to aid the weak author towards the powerful and strong producers and publishers. By way of the levies and the fixed distribution schemes of the collecting societies, the authors receive some financial compensation even if they out-licensed their entire rights to their works and waived any

¹¹³⁷ See: Art. 5 of the EU Directive; Sec. 45 et seq. of the German Copyright Act.

¹¹³⁸ Recitals to the German Copyright Act of 1985, BT Drucks. 10/837, p. 9.

¹¹³⁹ See: Schricker (1999): § 53, 3.

payment claims. By way of the levy systems, the legislators intend to strengthen the link between the author and his work and to ensure the author's constitutional right to receive a fair compensation for every exploitation of his intellectual property¹¹⁴⁰. It should be noted that this aspect was not taken into consideration by the European Commission in enacting the EU Directive. The EU Directive only looks to the relationship between users and right holders, not, however, to the relationship between right holders and authors.

III.3 Levies under the EU Directive

The EU Commission was not able to impose a European wide levy systems owing to the great differences in the existing national levy systems. As a compromise, the EU Directive states that in certain cases of exceptions or limitations — the member states being free to provide for such exceptions or limitations — the right holders should receive fair compensation to compensate them adequately for the use made of their protected works¹¹⁴¹. For other exceptions and limitations, the Member States may provide for fair compensation for right holders¹¹⁴². Specifically, right holders are to receive fair compensation for exceptions and limitations in respect of (i) reproductions on paper or any similar medium (Art. 5.2 (a) of the EU Directive), (ii) reproductions on any medium made by a natural person for private use (Art. 5.2 (b) of the EU Directive) and (iii) reproductions of broadcasts made by social institutions pursuing noncommercial purposes (Art. 5.2 (e) of the EU Directive).

III.4 Fair Compensation under the EU Directive

The EU Directive gives little guidance as to what considers fair compensation and how to calculate levy tariffs. Recital 35 states that

“When determining the [...] possible level of such fair compensation, account should be taken of the particular circumstances of each case [...] a valuable criterion would be the possible harm to the right holders resulting from the act in question. In cases where right holders have already received payment in some other form, for instance as part of a license fee, no specific or separate payment may be due. The level of fair compensation should take full account of the degree of use of technological protection measures [...] In certain situations where the prejudice to the right holder would be minimal, no obligation for payment may arise.”

Summarizing Recital 35, in assessing levies the Member States are to take into account the following.

¹¹⁴⁰ See: Schricker (1999): § 29, 4; BVerfG GRUR 1980, 44, 46 — Kirchenmusik; BGH, decision of July 11, 2002, GRUR 2002, 963 et seq. — Elektronischer Pressespiegel.

¹¹⁴¹ Recital 35 of the EU Directive.

¹¹⁴² Recital 36 of the EU Directive.

Possible Harm to Right Holders / Minimal Prejudice

The criterion of possible harm indicates that in certain cases no levy needs to be / should be assessed. An example could be television time shifting, arguing that such uses are of no or only minimal harm to right holders. Consequently, the industry argues that the Member States should not apply levies for such minimal harm uses. The EU Directive suggests that the competitive disadvantages resulting from different national levy systems may not justify the imposition of levies in these cases. Still, many Member States, including Germany, impose levies on time shifting and other minimal harm uses, e.g., by imposing levies on blank tapes.

Other Payments Received by the Right Holders

The criterion of other payments received by the right holders may direct to a “phasing out” of levy systems in the European Union. If the right holders receive license fees for certain uses under technological protection measure and digital rights management systems, they should not also receive a levy payment. For example, if a video recorder contains technological protection measures which requires the user to obtain a license before copying, irrespective of the statutory license granted for private use, no levy should have to be paid for such video recorder. Therefore, it can be argued that to the extent technological protection measures work or will work in the future no levies shall have to be paid.

The Use of Technological Protection Measures

One of the most discussed issues in the legislative process leading to the EU Directive was the relationship between levies on the one hand and technological protection measures on the other hand¹⁴³. Should levies have to be paid on equipment which provides for effective copy protection measures allowing individual licensing? Should copy protection measures be able to prohibit uses which are permitted by the exceptions and limitations of copyright?

The Commission gave priority to technological protection measures over levy systems. Levy systems should not hinder or disincentivize the development and use of technological protection measures.

According to Art. 5.2 (b) of the EU Directive, Member States shall consider the “*application or non-application of technological protection measures*”. Complimenting Art. 5.2 (b) and Recital 35, Recital 39 states that

“Member States should take due account of technological and economic developments, in particular with respect to digital private copying and remuneration schemes, when effective technological protection measures are available. Such exceptions or limitations should not inhibit the use of technological measures or their enforcement against circumvention.”

It is interesting to note that there is an inconsistency in wording between Art. 5.2 (b) referring to the application of technological protection measures and

¹⁴³ See: v. Diemar (2002): 587, 592; Günnewig within this book on page 528.

Recital 39 requiring only that technological protection measures are available. By electing “*application*” in the binding text of the EU Directive, the Commission suggests that right holders should continue to be compensated through levies even where technological protection measures are *available* but right holders choose not to use them. An example is copying from television broadcasting, as so far broadcasting companies are not making use of protection measures offered to them by the industry.

III.5 Levies under the German Copyright Act

The German Copyright Act requires the payment of levies for many of the statutory exceptions and limitations in Sections 45 et seq¹¹⁴⁴. The new Copyright Act to be enacted in April or May 2003 is likely to provide for additional exceptions and limitations and corresponding levy payments¹¹⁴⁵.

III.6 Equitable Remuneration According to the German Copyright Act

In consideration for the right to copy for internal and private use under Section 53 of the German Copyright Act, the author / creator is to receive *equitable remuneration* in consideration for the statutory licenses granted under Section 53 of the German Copyright Act¹¹⁴⁶. Sections 54 and 54 a of the German Copyright Act state:

“where the nature of a work makes it probable that it will be reproduced [...] in accordance with the [exceptions and limitations of copyright], the author of the work shall be entitled to payment of equitable remuneration from the manufactures of appliances and of video or audio recording mediums, that are intended for the making of such reproductions”.

There is, however, limited guidance on what is equitable, save that the amount of the levy “*shall depend on the type and extent of utilization of the equipment that is to be expected in view of the circumstances, particularly the location and the habitual use*”. In the absence of such guidance, it is unclear whether the “equitable remuneration” scheme under the German Copyright Act corresponds to the “fair compensation” scheme of the EU Directive. At present, the German legislator considers the two schemes to correspond and saw no need to change the general concept regarding levies in the new Copyright Act implementing the EU Directive.

The amounts of some levies are set forth in an Annex to Section 54 d of the German Copyright Act, others are being published by the German collecting societies, taking the tariffs in the Annex as a basis¹¹⁴⁷. Many of the levies in the

¹¹⁴⁴ See: Section 46, church and educational uses; Section 47 — school broadcasting; Section 49 — press clippings, Section 52 — certain public performances; Section 53 - copying for internal and private uses.

¹¹⁴⁵ See: Section 52 a — making available of works for educational and scientific purposes.

¹¹⁴⁶ See: Section 54 d of the German Copyright Act.

Annex are dating back to 1985. As a reaction to criticism that the levy tariffs are outdated and therefore no longer equitable, the German Government ordered the preparation of a report looking at the need to adopt copyright levies. The “Report of the German Government on the Development of Copyright Levies pursuant to Section 54 et seq. of the Copyright Act”¹¹⁴⁸ confirms that the tariffs for copyright levies are outdated and that there is a need to take action and that levies should be raised (rather than to limit the exceptions and limitations of copyright). It is therefore likely that the German legislator, in the near future, will increase the levy tariffs in the Annex.

Collecting societies have only rarely been disclosing studies, evaluations, calculations, comparisons or licensing schemes which they may or may not have used to come up with a specific tariff. Based on the EU Directive, in the future, equipment manufacturers and other parties subject to levy payments may oppose to levy tariffs arguing that the principles of the EU Directive on fair compensation have not been taken into consideration.

To implement the requirement under the EU Directive to consider the application or non-application of technological measures, the German legislator intends to amend the German Copyright Administration Act and to require the collecting societies to take into account technological protection measures when assessing levy tariffs (Section 13 (4) of the German Copyright Administration Act). Critics have argued that reference to technological protection measures should have been made in the Copyright Act itself and not only in the German Copyright Administration Act. Although speculative, it is not unlikely that the German legislator and German courts will give as little weight as possible to technological protection measures as they believe that levy systems are better suited to support authors.

IV Levies in the Digital Age

Digital reproduction techniques allow users to make vast numbers of perfect copies simply, quickly and cheaply. Copies made by digital technologies can no longer be distinguished from the original, they are said to be a clone of the original. The digital copying techniques in many cases substitute the traditional supply channels for works of authorship and thereby deprive both the right holders and the author of the compensation they were able to generate in the analogue world.

The differences between digital and analogue techniques and the consequences of such differences for right holders were the basis for enacting the EU Directive in the European Union and the Digital Millennium Copyright Act of 1998¹¹⁴⁹ in the United States. Both the EU and the US legislators had been confronted with

¹¹⁴⁷ The right to claim equitable remuneration exists irrespective of a set levy in the Annex to Section 54 d, BGH ZUM 1999, 649 — Telefaxgerät.

¹¹⁴⁸ See: 2. Vergütungsbericht dated July 11, 2000, BT-Drucksache 14/3972.

¹¹⁴⁹ See: www.loc.gov/copyright/legislation/dmca.pdf.

the question whether the exceptions and limitations of copyright should also apply to digital copies, or whether no or other — more narrow — exceptions and limitations should apply.

IV.1 Digital Copies under the EU Directive

The European legislator has seen the differences between analogue and digital technologies and has instructed the Member States to distinguish between the different technologies. One of the reasons given by the EU Commission to distinguish between analogue and digital technologies is that in the field of digital technologies differing national levy systems may have a negative impact on the functioning of the internal market. The EU Directive in Recital 38 states:

“Although differences between [the] remuneration schemes affect the functioning of the internal market, those differences, with respect to analogue private reproduction, should not have a significant impact on the development of the information society. Digital private copying is likely to be more widespread and have a greater economic impact. Due account should therefore be taken of the differences between digital and analogue private copying and a distinction should be made in certain respects between them.”

IV.2 Digital Copies under the German Copyright Act

The German legislator, however, contrary to Recital 38 of the EU Directive, positively affirms in Section 53 of the Bill of an amended German Copyright Act by which the EU Directive is implemented¹¹⁵⁰, that the exceptions and limitations of copyright apply to both analogue and digital copies, and makes no difference between the two technologies. The German legislator thereby confirms several decision of German courts, which have repeatedly held that the exceptions and limitations under the German Copyright Act also apply to digital copies¹¹⁵¹. In *Gema v. Hewlett–Packard GmbH*¹¹⁵² the Arbitration Board argued:

“The interest of the author cannot be protected by a prohibition of copying. Just as at the time of the framing of Sections 53 and 54 of the German Copyright Act in 1965, it is also not possible today to monitor and control private copying by digital means [...] There is no apparent substantive reason why, in relation to digital copying, the factual and legal implementation of a general prohibition should be judged differently. [...] Even assuming copy protection mechanisms were technically possible, this protection is irrelevant for the purposes of those audio and video data already on the market.”

¹¹⁵⁰ See: Bill of November 6, 2002, BT Drucksache 15/38.

¹¹⁵¹ e.g., BGH, decision of July 11, 2002, GRUR 2002, 963 et seq. — Elektronischer Pressespiegel; LG Stuttgart, decision of Juni 15, 2001, ZUM 2001, 711.

¹¹⁵² See: Decision of May 4, 2000 of the Arbitration Board, 21, 22.

The reasoning behind the position of the German legislator and the German courts is again that they believe the levy system to be best suited to support authors. Correspondingly, the collecting societies argue that the changes resulting from the digital technologies should lead to an increase rather than to a decrease of levies to compensate losses¹¹⁵³. This aspect was of critical importance in the decision of the Federal German Court (BGH) on electronic press clippings of July 11, 2002¹¹⁵⁴. The highest German Civil Court argued:

“The exceptions and limitations of copyright have to be — contrary to the general principle — construed broadly. For the construction of the exceptions and limitations it is relevant that such exceptions and limitations put the creator in a better position than he would be in under an exclusivity right [...] Section 49 of the Copyright Act effects that a significant part of the fees paid for press clippings goes to the creators of the work [...] An exclusivity right would not improve the position of the creators”.

The position of the German legislator is widely criticized. Legal scholars, producers, publishers and the IT industry argue that for digital equipment the levy system being a system of rough justice should be replaced by a system of technological protection measures and individual licensing¹¹⁵⁵. They, for example, promote to restrict the exceptions and limitations for digital uses to copies made from legitimate sources, rather than allowing to copy from the internet any material which has been unlawfully posted there. Furthermore, they suggest that digital copies should only be prepared by the user himself and it should not be permitted to have digital copies prepared by service providers¹¹⁵⁶. The requirement of legal access is also part of the EU Directive which states in Art. 6 (4) that *“Member States shall make available certain exceptions and limitations [...] where the beneficiary has legal access to the protected works”*. Still, the German legislator intends to also privilege copying from illegitimate copies, arguing that it is not reasonable for the user of such works to determine in each case whether the copy provided to him is in fact legal.

IV.3 Digital Copies under the Three Steps Test

There are good arguments to be made that in the digital world the system of exceptions and limitations of copyright and levies to compensate the statutory licenses are in violation of the so-called three steps test under the Berne Convention (Art. 9.2), the World Copyright Treaty (Art. 10.2) the TRIPS Agreement (Art. 13) and the EU Directive (Art. 5 (5)).

¹¹⁵³ See: Bericht des Rechtsausschusses, UFITA 129 (1995), 129.

¹¹⁵⁴ See: GRUR 2002, 963, 966 – Elektronischer Pressespiegel.

¹¹⁵⁵ See: Schack (2001b).

¹¹⁵⁶ See: Schricker (1999): § 53, 13; Loewenheim (2001): 415 ff.

According to the three steps test, limitations and exceptions of copyright shall

- (i) only be permitted in certain special cases,
- (ii) provided that the reproduction does not conflict with the normal exploitation of the work and
- (iii) does not unreasonably prejudice the legitimate interests of authors.

The three steps test requirements were met in the analogue world. The paper copy made from a book and the audio tape of a music clip did not conflict with the normal exploitation of the work. In the digital world this is no longer true.

IV.4 Levies on PCs, Printers, and Other Digital Equipment

In accordance with the German Copyright Act not differentiating between analogue and digital copies, the German collecting societies have started to impose levies on digital equipment and media.

German collecting societies have published tariffs for copyright levies on CD burners, PCs and printers. For example, VG Wort is claiming 30 Euros per PC¹¹⁵⁷ for the field of reprography and between €10 and €300 for printers. Regarding PCs, the notice states that

“PCs within the meaning of this notice are universal machines based on microprocessors with their own operating system (server and client) and storage facility, including all subcategories, such as, notebooks etc. Not subject to levies are: hosts (equipment which does not require an intelligent workstation) and workstations which do not have their own operating system, their own storage facility or any ability to undertake data exchange.”

Test cases have been brought by the collecting societies against Hewlett Packard regarding levies on CD Burner, against Fujitsu Siemens regarding levies on PCs and against Hewlett Packard regarding levies on printers. So far the IT industry has not been successful in any of these test cases to demonstrate that the respective equipment should not be subject to a levy under the Copyright Act.

The imposition of levies on PCs and printers by the German collecting societies is heavily criticized. First, it is argued that PCs are rarely used to copy copyright protected materials. Typically PCs are used to create and modify own documents. If third party documents are being used, in most cases such third party has expressly or implicitly permitted the use of his work. Any such use does not require the statutory licensing scheme under Sections 53 et seq. of the German Copyright Act.¹¹⁵⁸

Further, the industry points out that levies are already being paid for other IT equipment such as CD burners and scanners. The imposition of levies on

¹¹⁵⁷ See: Bundesanzeiger of December 21, 2000.

¹¹⁵⁸ The collecting societies have ordered a study on private and business uses of PCs which states that 27% of all private uses and 43% of all business uses of PCs refer to third party content, GfK Panel Services Consumer Research GmbH, available at: <http://www.vgwort.de/files/GFK04.htm>.

PCs first by VG Wort, later by ZPÜ, the imposition of levies on printers, hard discs, RAM storage media would overly burden the IT industry and would end in excessive payment obligations. They point to the decision of the German Federal Court (Bundesgerichtshof) in its decision of 2001 on levies imposed on scanners¹¹⁵⁹ stating:

“If equipment can only be used for copying in connection with other equipment, levies shall not have to be paid on all appliances which are part of such copying unit.”

Regarding scanners the Federal Court held that in the copying unit consisting of scanner, PC and printer, the scanner is the one appliance which is directly used to operate as copying equipment.

Finally, the opponents point to other European countries. As Germany is the only country imposing levies on PCs, it is likely that consumers will purchase their PCs in other countries which may lead to a severe competitive disadvantage of the German IT industry and trade.

¹¹⁵⁹ See: BGH, decision of July 4, 2001, BGH GRUR 2002, 246 — Geräteabgabepflicht.

4.2.4 Tipping the Scale in Favor of the Right Holders: The European Anti-Circumvention Provisions

*S  verine Dusollier*¹¹⁶⁰

Abstract: The European directive on the copyright in the information society provides for some provisions against circumvention of Digital Rights Management technologies. Circumventing a technological measure or making and trafficking in circumvention tools are now prohibited activities in the European Union. Despite the expressed intention of the European lawmaker to safeguard a balance between the rights of the copyright holders and the interests of the users and society at large, the anti-circumvention provisions give the rights owners preference: the protection is broad and surely extends beyond the boundaries of copyright; the exceptions are overridden, albeit the empty promise of the article 6(4). The scale has been here mostly tipped in favor of the economic interests of the authors. This paper describes the anti-circumvention provisions of the directive and the new (im)balance they put in place.

I Introduction

On the 22 May 2001, the European Council has finally adopted the directive on the harmonisation of certain aspects of copyright and related rights in the information society¹¹⁶¹. This directive completes a process of harmonization of copyright and related rights amongst the Member States and of adaptation of copyright to the information society, that has been engaged in as early as 1995 with the Green Paper of the European Commission on copyright in the information society¹¹⁶². The directive also implements the WIPO treaties of 1996, as the United States have done in 1998 with the Digital Millennium Copyright Act. Six topics have been considered as requiring a Community intervention for harmonization: the right of reproduction, the right of communication to the public, the right of distribution and the extent of its exhaustion, the exceptions to copyright and related rights, the technological measures of protection and the rights management information.

This article will consider only one of those topics, that of the legal protection of technological measures, otherwise called the anti-circumvention provisions. It was certainly one of the key issues in the negotiations that have led to the adoption of the directive. The controversy surrounding such protection, and notably the relationship between technical lock-ups and limitations to copyright, was so intense it was nearly the breaking point of the whole directive. It kept being a contentious issue until the end when the Commission finally brought a proposition for a solution concerning the preservation of the exceptions.

The solution, as enacted in article 6 paragraph 4 of the directive, is but a delicate compromise between the friends and the foes of an absolute legal protection. As

¹¹⁶⁰ University of Namur (Belgium).

¹¹⁶¹ See: Directive 2001/29/EC.

¹¹⁶² See: Green Paper (1995).

any compromise, it is built on intricate and cryptic provisions. Legal scholars, let alone students, will likely have a hard time understanding their meaning. The compromise is also a delegation to Member States since the ultimate outcome of the article 6 will be that the national lawmakers will have to find the panacea to the conflict between technological measures and copyright limitations.

The anti-circumvention provisions are laid down in the article 6 of the directive that states:

1. Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective.
2. Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which:
 - a) are promoted, advertised or marketed for the purpose of circumvention of, or
 - b) have only a limited commercially significant purpose or use other than to circumvent, or
 - c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of,
 any effective technological measures.
3. For the purposes of this Directive, the expression “technological measures” means any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorised by the rightholder of any copyright or any right related to copyright as provided for by law or the sui generis right provided for in Chapter III of Directive 96/9/EC. Technological measures shall be deemed “effective” where the use of a protected work or other subject-matter is controlled by the rightholders through application of an access control or protection process, such as encryption, scrambling or other transformation of the work or other subject-matter or a copy control mechanism, which achieves the protection objective.
4. Notwithstanding the legal protection provided for in paragraph 1, in the absence of voluntary measures taken by rightholders, including agreements between rightholders and other parties concerned, Member States shall take appropriate measures to ensure that rightholders make available to the beneficiary of an exception or limitation provided for in national law in accordance with Article 5(2)(a), (2)(c), (2)(d), (2)(e), (3)(a), (3)(b) or (3)(e) the means of benefiting from that exception or limitation, to the extent necessary to benefit from that exception or limitation and where that beneficiary has legal access to the protected work or subject-matter concerned.

A Member State may also take such measures in respect of a beneficiary of an exception or limitation provided for in accordance with Article 5(2)(b), unless reproduction for private use has already been made possible by righthold-

ers to the extent necessary to benefit from the exception or limitation concerned and in accordance with the provisions of Article 5(2)(b) and (5), without preventing rightholders from adopting adequate measures regarding the number of reproductions in accordance with these provisions.

The technological measures applied voluntarily by rightholders, including those applied in implementation of voluntary agreements, and technological measures applied in implementation of the measures taken by Member States, shall enjoy the legal protection provided for in paragraph 1.

The provisions of the first and second subparagraphs shall not apply to works or other subject-matter made available to the public on agreed contractual terms in such a way that members of the public may access them from a place and at a time individually chosen by them.

When this Article is applied in the context of Directives 92/100/EEC and 96/9/EC, this paragraph shall apply *mutatis mutandis*.

The first two paragraphs deal with the activities to be prohibited by the Member States: the circumvention of a technological measure on the one hand, the trafficking of devices enabling such a circumvention on the other hand. A next Section of this article will consider this twofold prohibition. Beforehand, the first section will turn to the definition of the technological measures to be protected by the article 6 of the Directive, as described in its paragraph 3.

The paper will then give an overview of the most intricate provision of the directive, which deals with the exceptions facing the technological measures. Laying down some rules to safeguard exceptions in a technologically protected copyright world, article 6(4) doubtless is the most important and perhaps revolutionary part of the directive. A great part of this article will be devoted thereto and analyze thoroughly the intents and results of this desire towards a balance.

ak finally, the directive also comprises several other provisions regarding the technological measures. Some are hidden in the recitals of the directive¹¹⁶³, some in other articles than article 6. They might in some cases establish key or odd principles in that field. The last Section will examine these diverse provisions.

It is worthwhile to note — and it could be of some interest to persons who are not accustomed to the European legislative process — that an European directive is not in force by itself. It constitutes only some basic provisions that the Member States are obliged to transpose in their laws. Therefore, the provisions

¹¹⁶³ Recitals of European directives have no mandatory nature by themselves. They normally serve as helping the interpretation of the provisions of the directive. They should not be transposed as such by the Member States when implementing the directive. Nevertheless, they are increasingly used as a vehicle for additional or accessory rules. The directive on the copyright in the information society includes some key provisions in its recitals. It is unclear whether the Member States have to take them into account. Since they have to implement an appropriate protection of technological measures, some rules of the recitals could play a role in considering the appropriateness of the protection. For instance, as far as limitations to copyright are concerned, “appropriate” should mean a balanced protection. Therefore the limitations laid down in the recitals should be considered by the national legislators.

as appearing in the directive of 2001 and as explained below, will not be of direct application in the Member States. The latter are only obliged to transpose in their regulatory framework the principles of the directive, when needed. They are free to do so in any way that is not incompatible with the objectives and principles of the adopted directive. As a consequence, the national regulatory frameworks that will emerge from the transposition process might be slightly different than the provisions of the article 6¹¹⁶⁴. Besides, only the fields where a need for harmonization is needed so as to ensure a smooth functioning of the internal market are open for directives at the European level. That explains that the anti-circumvention provisions laid down in the directive do not comprise any remedies, which are traditionally considered as a matter for Member States' authority.

II Object of the Protection

Technological measures to be protected against both circumvention and trafficking of circumventing devices are defined in article 6(3) as: "*any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorized by the rightholder of any copyright or any right related to copyright as provided for by law or the sui generis right provided for in Chapter III of Directive 96/9/EC*".

Such a definition is very broad. It covers any technical tool used by a copyright owner to protect her work and the distribution thereof. The key element here is the restriction of acts which are not authorized by the rightholder. The anti-circumvention provisions laid down in the directive vest any device that conveys in the practice — in the machine — a lack of authorization of the author. This makes the protection of article 6 larger than that in the prior versions of the European text. The draft proposal of 1997 only dealt with technological measures designed to prevent or inhibit the infringement of any copyright or any rights related thereto. At first sight, that meant that only the devices aiming at following the contours of the exclusive rights of the author or holder of a neighboring right were concerned¹¹⁶⁵. The technically granted monopoly had to be rather similar to the legally granted one. One straight example is the anti-copy

¹¹⁶⁴ One good example of the somewhat diverse transpositions is the implementation of the 1991 software directive and of its provisions on technological measures. The picture of the Member States was fairly rainbowed, from countries that transposed the very wording of the prohibition of circumvention devices in the field of computer programs, to countries where the existing regulatory framework has been considered as offering an adequate protection. France has done so and justified the lack of a specific provision related to anti-circumvention devices, save for a peculiar publicity obligation, by asserting that the general regime and case law governing aiding and abetting copyright infringement could sufficiently cover the prohibition of circumventing devices.

¹¹⁶⁵ Nevertheless, other types of measures could have been covered given the definition of the effectiveness of such measures. See *infra*.

device whose primary function is to apply the exclusive right of reproduction. The adopted version of the directive goes largely further. Technological measures restricting any activities included in the legal ambit of the copyright are protected, as well as any mechanism inhibiting uses not accepted by the copyright owner, even though such uses are not per se restricted by the legal monopoly. It suffices that the copyright owner forbids by contract one use or another so that the technological measure that applies her will, is protected by article 6.

Even the Digital Millennium Copyright Act does not go so far. Apart from technological measures that protect a right legally granted by the Copyright Act, the protection extends to measures that grant access to works, such measures being clearly circumscribed.

In the European directive, the technological measures shall only be deemed effective — and as a consequence covered by the protection — “*where the use of a protected work or other subject-matter is controlled by the rightholders through application of an access control or protection process, such as encryption, scrambling or other transformation of the work or other subject-matter or a copy control mechanism, which achieves the protection objective*”.

A first comment here is that such a formulation might appear rather circular. The technical protection will be considered as effective only when its process “achieves the protection objective”. According to Pierre Sirinelli, this construction would destroy the whole system¹¹⁶⁶. As Sirinelli, I don’t think this provision should be read as requiring an infallible lock-up. Anyway, such wording remains very ambiguous. Rather than giving sense to the effectiveness criterion first laid down by the WIPO Treaties, the European lawmaker, as the DMCA drafters for that matter, has only used that element as a precision of the definition of the technological measures to be protected.

Effectiveness will be namely met when an access control is applied. A lot has been said about this surprising consequence of the protection of technical measures controlling access to works being that such protection might lead to grant a new right to copyright holders, i.e. the right to control access to works¹¹⁶⁷. This new ‘de facto’ right goes beyond the criteria of exercise of their rights which justified the protection of technological measures enacted by the WIPO Treaties. In our opinion, granting access to her works is not — and should not be — as such an exclusive right granted to the author by copyright law. Anti-circumvention provisions that include such a technical feature in the copyright regime dramatically shift the underlying paradigm of the protection of literary and artistic works. For sure, it might be the end of the copyright world as we know it.

The 1997 proposal for the information society directive only referred to the control of access to works as far as effectiveness was concerned¹¹⁶⁸. Were this first

¹¹⁶⁶ See: Sirinelli (2001).

¹¹⁶⁷ Controlling access to works being included in the copyright ambit is still fiercely discussed. See: Ginsburg (2000); Hansen (2000); Heide (2000): 993–1048; Koelman, Helberger (2000): 174; Dusollier (2000): 25–52.

¹¹⁶⁸ See: Dusollier (1999): 285–297.

version be adopted, some technical measures would have been left out of the Directive. For instance the Serial Copy Management Systems, or the mere anti-copy devices, or even some digital right management systems which would be designed or programmed only for usage-tracking purposes. In such cases where the access is not the main objective of the technological measure, it could have been feared that the device would not be entitled to benefit from the protection¹¹⁶⁹. In the legislative process, the European Parliament has put the control of the use of the copyrighted work aside the ‘access’ element. That covered more largely any type of technological measures, whatever they controlled access to, copy or any other use of the work. In the finally adopted directive, only the ‘use’ element remains. This clearly covers a whole range of electronic protection tools. Though, the scope of the protection granted by such a wording (‘use’) is fairly extensive, along with what the first alinea of this paragraph has showed. Any device that restricts any use of the work, from the access thereto to any eventual enjoyment of the work, is deemed as effective, hence entitled to the ban on circumvention activities.

As I have seen earlier, since the definition of technological measures does not strictly relate to copyright infringement but also to any use against the private will of the copyright holder, it confirms that as soon as the access to the work is restricted by the author, the technical lock-up conveying this will is protected by the anti-circumvention provisions.

Finally, the definition precise that effective protection processes encompass encryption, scrambling¹¹⁷⁰ or other transformation of the work or other subject-matter or a copy control mechanism. One major mistake has thus been corrected. Earlier versions of the directive said that the technological measures to be protected were effective processes including decryption or descrambling, which were precisely the activities against which the protection was directed. The adopted text is now more adequate by providing that encryption and scrambling are amongst the protected technologies. This highlights once again that access controls are clearly belonging to the protection scope.

III The Scope of the Prohibition

III.1 Circumvention Act v. Circumvention Devices

The 1997 proposed directive prohibited any “activities” of circumvention, some of them, e.g. the sale or rental of circumvention devices, being unexhaustively listed. The very act of circumventing a protection mechanism was not clearly outlawed. Since 1999, successive versions of the directive, have stressed a plain distinction between the circumvention and the trafficking of circumventing devices, both being prohibited. Now the first paragraph of article 6 prohibits the

¹¹⁶⁹ See: *ibidem*.

¹¹⁷⁰ This sufficiently demonstrates that the directive is primarily concerned with encryption and other access controls.

circumvention of technological measures while the second one deals with the trafficking of any devices enabling or facilitating the circumvention.

Let's start with the circumvention. A former version of the directive provided that the circumvention had to be unauthorized by the rightholders. This condition has faded away albeit the lobbying of some rightholders in favor of this non-authorization requirement. As a matter of fact, one can wonder to what extent this precision could have better served the interests of the copyright holders. It seems rather logical that the prohibition applies only where the circumvention is not duly authorized by the authors.

The provision does not repeat anymore that the technological measure whose circumvention is prohibited, aims at protecting the copyright, related rights or the sui generis rights applied to databases. Since the object of the protection is fully defined in the paragraph 3, the clearing up of the text makes it less intricate.

As far as circumvention is concerned, an intent requirement has nevertheless been added. Only the person carrying out in the knowledge, or with reasonable grounds to know, that he or she is pursuing the objective of circumventing a technological measure could be held liable under article 61 of the directive. Such a knowledge is not required in the anti-trafficking provision.

The prohibition of activities related to circumventing devices is very broad. Should be prohibited or regulated by the Members States when implementing the directive the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of unlawful devices¹¹⁷¹. The provision of services of circumvention is mentioned as well. As a consequence, most trafficking in activities should be covered. Nevertheless, the directive does not add a safeguard clause of the type of the section 1201(a)(2) of the DMCA that further prohibits the "otherwise trafficking in". The list of activities in article 6 is thus closed. However, one recital¹¹⁷² provides that legal protection of technological measures is without prejudice to the application of any national provisions which may prohibit the private possession of devices, products or components for the circumvention of technological measures. The scope of the prohibited activities related to circumvention devices could thus be broader in some countries so as to include the private possession of such devices.

The activities to be prohibited are the same than those prohibited by another key directive in the field of anti-circumvention: the directive on the legal protection of services based on, or consisting of, conditional access¹¹⁷³. The conditional access directive¹¹⁷⁴ covers radio or television broadcasting services and information society services, normally defined in European Union legislation as "any service normally provided for remuneration, at a distance, by electronic means

¹¹⁷¹ The unlawfulness of the devices will be considered below.

¹¹⁷² See: Recital 49 of the Directive.

¹¹⁷³ See: European Parliament and Council Directive 98/84/CE.

¹¹⁷⁴ For a complete overview of the directive, see: Helberger (1999): 88.

and at the individual request of a recipient of services”¹¹⁷⁵. The main purpose of this directive is to prohibit trafficking in devices that could circumvent a conditional access service¹¹⁷⁶. Therefore, it presents a close relationship with copyright-related anti-circumvention provisions. The implications of this link between both fields, though largely overlooked in the early days, are now regularly addressed by legal scholars¹¹⁷⁷. The similarity of activities to be prohibited in both directives proves that the European lawmaker has clearly seen the likely relationship between both texts.

III.2 Unlawful Devices

The illegitimacy of the devices, products or components as related to their potential use as a circumvention tool is determined by three alternative criteria. Either the device is promoted, advertised or marketed for the purpose of circumvention, or has only a limited commercially significant purpose or use other than to circumvent, or is primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of any effective technological measures. Criteria to be met here are pretty similar to those of the DMCA.

As a practical matter, the provision covers devices that are clearly intended to serve as a circumvention tool. The commercial asset of such devices should reside in this probable use. Therefore, the design or the marketing of the product primarily stress this circumvention function.

This does not mean that considering the unlawfulness of some multipurpose devices will be an easy task. At the end of the day, only the courts will decide whether one particular device is legitimate or not. The “primary purpose” criteria, if it seems more balanced than the “sole intended purpose” that has been sometimes put forward¹¹⁷⁸, does not settle the matter in a definitive way. The determination of the threshold of a primary purpose, between infringing and not-infringing uses that multi-purposes devices could enable, is still to be made.

¹¹⁷⁵ See the Article 1(2) of Directive 1998/34/EC: p. 23.

¹¹⁷⁶ Protection applies to services on two conditions. The first one is that the service is based on a conditional access, which is defined as “any technical measure and/or arrangement whereby access to the protected service in an intelligible form is made conditional upon prior individual authorisation”. The directive also covers the provision of conditional access to the above services, considered as a service in its own right. Thus both the service provided upon conditional access and the technique or the service granting such access are concerned. The second condition is that the purpose of conditional access is to ensure the remuneration of the service.

¹¹⁷⁷ See: Heide (2000): 993–1048; Koelman, Helberger (2000): 174.

¹¹⁷⁸ See the Software directive. Thomas Vinje was a strong proponent of the sole intended purpose criteria, see: Vinje (1996): 431–440.

III.3 The Prohibition within or outside of Copyright Regime

According to the subsidiarity principle, the Member States should be free in the manner to implement the anti-circumvention provisions of the directive in their own regulatory framework, as long as the objective of the directive is met and the competition in the internal market is not distorted. In our view, nothing prevents Member States from enacting the anti-circumvention regime out of copyright, for instance in a separate piece of legislation.

Countries could indeed decide to implement the WIPO Treaties obligations on technological measures in fields of law other than in copyright,¹¹⁷⁹ e.g., in conditional access regimes, unfair competition laws or computer crime regulatory framework. The 1996 Treaties do not forbid it¹¹⁸⁰. What WIPO, and the European directive, only require is that the protection be adequate.

However, the easily-overlooked article 8 of the directive limits this freedom of manoeuvre. It states that each Member State shall take the measures necessary to ensure that rightholders can bring an action for damages and/or apply for an injunction and, where appropriate, for the seizure of infringing material as well as of circumventing devices. The legal field in which the anti-circumvention provisions will be placed should therefore include such remedies and sanctions. For example, this will not be the case for computer crime legislation.

IV Boundaries of Copyright

Technical locks can jeopardize the legitimate exercise of exceptions to copyright and the whole balance of the copyright regime. That song has been largely heard. It was a key issue to be solved by the European law-maker that has finally stated its solution in the fourth paragraph of the article 6 of the directive.

Compared to other anti-circumvention provisions around the world, the European ones distinguish themselves in the manner they face the issue. Indeed, while the United States or Australia have only considered the solution to that 'fair use' issue at the level of the sanction for circumvention, the European Union has chosen to rule the matter even before the enforcement stage. The former countries have enacted different safeguard mechanisms but both exempt the user when the circumvention she carried out was in the framework of the legitimate exercise of

¹¹⁷⁹ Opponents to the anti-circumvention provisions in copyright have sometimes argued that new protection was useless since other existing regimes could offer sufficient protection and meet the concern of right holders. According to scholars, the adequate protection was to be found in computer crime, unfair competition law or European conditional access protection. See: Koelman, Helberger (2000): 222. Japan, for instance, separates anti-circumvention of technical measures protecting rights of the authors, laid down in the copyright act, from anti-circumvention of access controls that it regulates under unfair competition law. Different legal techniques respond to two different protection features.

¹¹⁸⁰ Intervention of Kurt Kemper, Workshop on the WIPO Treaties, 6-7 December 1999, Geneva.

some exceptions¹¹⁸¹. In such a case, the legitimate use being technically locked-up, the user has no choice but to circumvent the digital protection. The US law does not give her the tools to do so but will not hold her liable in some, albeit strict, conditions. The Australian law also grants a non liability in that case to providers of the circumvention means. The message here is thus: “circumvent—we-do-not-sue”. It does not actually solve the issue of the digital lock-up. While in the analogue environment the copyright exemption was primarily used as a defense in litigation for copyright infringement whatever its success might be, in a digital world wrapped by technological devices, the function of exemptions system will be completely different. If any act of reproduction or communication of a copyrighted work is inhibited by a technological protection, the user will have either to sue the rightholder for enabling her to exercise her exemption (for instance for research, education, criticism purpose); either to deploy some skill for circumventing the technical measure. In both cases, the burden imposed on the user is rather heavy. The solution put forward by the DMCA and the Australian Copyright Act resumes the function of the exception as a defense only in the case of an action brought against the user for having circumvented the system. (or against the provider of a device in the Australian case for having distributed the device). Both solutions do not seek to reduce the technological restraint on the legitimate exceptions. This is what the directive tries to achieve. Indeed, the European directive seeks to put the balance in favor of the user not at the stage of the sanctions for circumvention, but at the earlier stage of the very exercise of the exception constrained by a technical measure. To this end, the directive puts forward an intricate provision, the article 6(4).

The first principle laid down in this article is to entrust the rightholders with the task of reconciling the technological measures with the safeguarding of the exceptions. The first indent of 6(4) states: “*in the absence of voluntary measures taken by rightholders, including agreements between rightholders and other parties concerned, Member States shall take appropriate measures to ensure that rightholders make available to the beneficiary of an exception or limitation, the means of benefiting from that exception or limitation, to the extent necessary to benefit from that exception or limitation and where that beneficiary has legal access to the protected work or subject-matter concerned*”. The intervention of the lawmaker is therefore subsidiary to that of the authors and other rights owners.

¹¹⁸¹ Yet, both systems are largely different. The US DMCA does not held liable the circumventer in very limited cases (such as reverse engineering, security testing, etc.) that do not run parallel to the copyright fair use and when the technological measures protects an exclusive right. Furthermore, generally the exceptions to anti-circumvention provisions — or the ‘fair hacking’ rights, as Jane Ginsburg has qualified them — only applies to the circumvention itself and not the trafficking in circumvention devices. Conversely, the Australia does not prohibit the circumvention itself but the trafficking in the circumvention devices. The fair use concern is thus limited. Anyway, the Australian regime enables the trafficking in circumvention devices where the user who will use the device, signs a declaration that the device will be only used for an identified permitted purpose. On the Australian provisions, see: de Werra (2001); Fitzpatrick (2000): 214–228.

Preference is given to any voluntary measures taken by rightholders. The State should intervene only in default of such measures. The directive does not define the ‘voluntary measures’, save for mentioning agreements between rightholders and other parties concerned. As examples, the rightholders could devise or revise the technological measures so as to accommodate some exceptions or put in a place some breathing space in favor of the user; provide some ‘big’ users with unlocked copy of the works or apply alternative pricing policy¹¹⁸². Rather than the safeguarding of the exceptions and limitations of copyright, the freedom to contract of the authors is here privileged. The exception is clearly to be contracted¹¹⁸³. Such a principle stands along the solution advocated by Tom Bell who considered the “fair use” to become “fared use”¹¹⁸⁴ so as any exception could be licensed and paid for. What remains of the exception, whose key principle is to skip the need for an authorization of the rightholder, in such a bargaining?

In default of such measures from rightholders, the Member States are obliged to take “*appropriate measures to ensure that rightholders make available the means of benefiting from [some] exception[s]*”. But nothing indicates when the default from the side of the rightholders will be sufficiently patent as to necessitate that the State takes the stage. It should be stated in the national implementation of the directive, the period of time at the expiration of which, if no measures have been taken by rightholders, the State must intervene, and the criteria for considering the appropriateness of the measures taken by the authors. On the latter, the directive prescribes nothing. Yet, the State should be allowed to address the merits of the measures taken by the rightholders before considering its intervention. Would any measure, even minimal, free the State from its legislative duty to safeguard the public interest, it would give too much of a unrestrained power to the authors.

The purpose of the appropriate measures to be taken by the States is to make available to the users the means of benefiting from exceptions. Such means should be made available only to beneficiaries of exceptions who have legal access to the protected work. This does not mean that the access to works should be granted to such users. Only the persons who have already access to works should be empowered to exercise legitimate exceptions. The case referred to here is when a work that has been legitimately purchased (or when the access thereto has been legitimately gained in whatever manner) is technically protected to the extent that some legitimate uses cannot be accomplished. For instance, a technical lock-up over a CD ROM on the history of the United States, rightfully purchased by a teacher, could prevent her from any copy for use in the classroom. Or a library would be restrained to make an archival copy of a database it has paid for. Article 6(4) is not about granting a free access to users.

¹¹⁸² Those are some measures mentioned by The International Federation of Phonograms Industry (IFPI).

¹¹⁸³ That is reinforced by the reference to ‘agreements’.

¹¹⁸⁴ See: Bell (1998): 558–618.

The directive does not give any indication about the type of appropriate measures the Member States could take, nor how the Commission will consider the appropriateness of the taken measures, hence the proper implementation of the directive. Leaving the freedom to States to decide which measures could be appropriate to safeguard the exceptions was likely a way to get rid of this tricky issue; it will also be a likely failure of the objective for harmonization amongst Member States. Should rightholders make their technically protected works and products compliant with different measures from one country to another, it would certainly not help a smooth functioning of the Internal Market.

This favor to users is only granted to some limited exceptions¹¹⁸⁵. These are the exceptions in respect of reproductions on paper or any similar medium or reprography (article 5 (2) a), in respect of specific acts of reproduction made by publicly accessible libraries, educational establishments or museums, or by archives (article 5 (2) c), in respect of ephemeral recordings of works made by broadcasting organizations (article 5 (2) d), in respect of reproductions of broadcasts made by social institutions pursuing non-commercial purposes (article 5 (2) e), the use for the sole purpose of illustration for teaching or scientific research (article 5 (3) a), uses for the benefit of people with a disability (article 5 (3) b) and the use for the purposes of public security (article 5 (3) e). The private copy exception enjoys a specific regime I will consider later on.

Neither the directive, nor the legislative history explain why some exceptions have been elected to this favoring regime while others have not. It has been said that these were exceptions that conveyed strong public interests, such as fundamental freedoms. Yet, neither the exception of parody, which is a persuasive illustration of the freedom of expression concern, nor the exception for news reporting, which translates the concern of the freedoms of information and of the press, are included in the restricted list of article 6(4). One could also explain the criteria having lead to the choice of some exceptions by the fact that the user of each exception is easily identifiable, which could make it easier to establish a contractual relationship between the user and the rightholder. Some exceptions of the list indeed relate to identified user such as the libraries and archives, the broadcasting organizations, the educational establishments, some social institutions, or administrative offices. But the argument is not convincing altogether. What about the reprography exception whose users are potentially any member of the public? Why is the news reporting exception, whose beneficiaries, i.e. the press and reporters, could be easily identified, not included in the list then?

Member States should take appropriate measures only for exceptions listed in article 6(4) to the extent such exceptions exist in their regulatory framework. We have seen that the list of exceptions allowed in the article 5 of the directive

¹¹⁸⁵ It should be reminded that the directive states a long list of 23 exceptions whose only one (i.e. the exception for temporary acts of reproduction) is to be mandatorily implemented in the regulatory framework of the Member States. Other exceptions are what some have called a 'shopping list' in which Member States can choose. So much for the harmonization purpose marketed by the Commission. See: Hugenholtz (2000a): 499–502.

was only optional. Therefore, if one exception of article 6(4) has not been chosen by a country to be part of its copyright regime, it does not make sense to grant the exception to users in the case of a technological restraint. For instance, France does not know any education or research-related exceptions. This should not change when implementing the directive. The French legislature will not be obliged to make available to educational institutions the means to benefit in the practice from an exception that does not exist in the law. This underlines the strangeness of the whole article 6(4) that makes mandatory the safeguarding of exceptions whose enactment itself is not.

But the provision of article 6(4) has to benefit also to similar exceptions that could exist in the related rights and *sui generis* right regimes.

The second indent of the article 6(4) provides for a similar solution (appropriate measures of the States if rightholders fail to do so) as far as private copy is concerned. In that case, the intervention of the legislator is not mandatory, but optional. Here also, the initiative lies on the rightholders who can namely put in place serial copy management systems allowing for one or a small number of copies. The directive requests from Member States not to prevent rightholders from adopting such measures. The directive states further that all technological measures either applied voluntarily by rightholders, including those applied in implementation of voluntary agreements, or applied in implementation of the measures taken by Member States, shall enjoy the legal protection provided for in paragraph 1. Such a precision is not useless. Otherwise, some defendants having circumvented the serial copy management systems, could argue that, since the technological measure aims at guaranteeing a private copy exception, it does not comply with the definition of the measure, as laid down in article 6(3), that qualify the measure as aiming at restricting an unauthorized act. It would be of course a somewhat distorted defense.

The fourth indent of 6(4) might be the greatest defect of the whole construction. It says that the provisions of the first and second subparagraphs [i.e. the obligation to take some measures to safeguard some exceptions] shall not apply to works or other subject-matter made available to the public on agreed contractual terms in such a way that members of the public may access them from a place and at a time individually chosen by them.

The wording of this provision plainly refers to the definition of the right to make works available to the public, as laid down in article 3 of the directive. It would mean that any on-demand service will not have to comply with the obligation to safeguard the exceptions and could be completely locked up. One case put forward by the music industry is the making available of music for a limited time, e.g. for the duration of one weekend where you plan to have a party. According to the IFPI, enabling some exceptions, such as the private copy, would ruin this new business model of distribution, and thus the normal exploitation of the work.

The vagueness of the wording could nevertheless jeopardize all the good intents of article 6(4). Making available works on the Internet could become the prevalent business model for distribution of works. The requirement that such services have

to be delivered on contractual terms does not matter much given the easiness to embed a click-wrap license in digital products. Some commentators have expressed concerns about this paragraph that could comprise the whole Internet and make void any obligation for preserving some exceptions. I share those views.

Another provision of the directive tends to promote the balance between the exceptions and the risk of a technical lock-up. The article 12 asks the European Commission to examine the implementation and effects of some provisions of the directive. As far as article 6 is concerned, the Commission will have to consider whether acts which are permitted by law are being adversely affected by the use of effective technological measures. The wording here reminds of that of the US DMCA that entrust the Library of Congress with a similar rulemaking. In the European context, the rulemaking will be less direct, since the Commission, as a result of such a consideration, can only propose some amendments to the directive to be finally decided by the European Council and Parliament.

V Miscellaneous

V.1 Exemptions of Liability for Circumvention Activities

Contrary to the DMCA, the European directive does not provide for a list of exceptions to the prohibition of circumvention or to the ban of circumventing devices. Nevertheless, some recitals of the directive state that the protection should not hinder research into cryptography¹¹⁸⁶. It should neither inhibit nor prevent the development or use of any means of circumventing a technological measure that is necessary to enable reverse engineering or the testing of the good functioning of computer programs¹¹⁸⁷, as authorized by the articles 5(3) and 6 of the Directive 91/250/EEC. Circumventing a technological measure, or developing means to do so, will be allowed when the purpose is to reverse engineer the technically-protected program¹¹⁸⁸.

The legal force of such exceptions as included in the recitals, is not plain. Even though recitals can only serve as interpreting tools of the directive itself, one could argue that if a Member State has not implemented an exception for reverse engineering, it has not properly transposed the directive since the legal protection it has enacted is not proportional.

V.2 No Mandate

Some technical protection mechanisms require the compliance of the players or reproduction devices. A signal or, as it is sometimes called, a “flag” is then

¹¹⁸⁶ See: Recital 48 in fine.

¹¹⁸⁷ See: Recital 50.

¹¹⁸⁸ The reverse engineering will have to comply with the conditions laid down in the software directive of 1991, i.e., it should be carried out by a legitimate user and the informations necessary to achieve the interoperability are not in any other way available. The purpose of the reverse engineering, and this of the circumvention needed in that purpose, should be to achieve the interoperability.

embedded in the digital code of the work and sent to the player device for recognition. When the device acknowledge such signal, it can inhibit the copy, printing, or access to works. The electronic consumer manufacturing industry did not want to be obliged to devise their products in such a way that they comply with any technical protection scheme on the market. Therefore, it asked, as in the DMCA, a no mandate clause clearly stating that no such obligation lies upon it. The no mandate clause appears in the recital 48 that confirms that there is “no obligation to design devices, products, components or services to correspond to technological measures, so long as such device, product, component or service does not otherwise fall under the prohibition of Article 6”.

The same recital reassures the electronic consumer manufacturing industry about the necessity to preserve the playability of the works on their devices. The technological systems put in place by copyright holders should not prevent the normal operation of electronic equipment and its technological development.

V.3 Acquis Communautaire and the Software Directive

The software directive of 19 May 1991¹¹⁸⁹ is the first piece of enabling legislation which has ever provided a legal protection of anti-copy devices in Europe. The article 7 1 (c) of the software directive stated that “[...] *Member States shall provide [...] appropriate remedies against a person committing [...] c) any act of putting into circulation or the possession for commercial purpose of, any means the sole intended purpose of which is to facilitate the unauthorized removal or circumvention of any technical device which may have been applied to protect a computer program.*” The protection contained herein is mostly similar in Member States legislation having transposed the Directive.

The information society directive contains a rather odd provision. Indeed its recital 50 provides that “[the] *legal protection [of technological measures] does not affect the specific provisions on protection provided for by Directive 91/250/EEC. In particular, it should not apply to the protection of technological measures used in connection with computer programs, which is exclusively addressed in that Directive*”.

As a consequence, circumvention activities should only be prosecuted on the grounds of the national provisions having transposed the article 7(c) of the software directive. This article did only cover the trafficking in devices and not the circumvention itself. Furthermore, only the devices whose sole intended purpose was the circumvention, and only the commercial activities related to such devices are unlawful under the 1991 directive. The protection for technological measures applied to software is thus less than for other types of works. It would have been logical to delete the article 7(c) of the software directive and to provide the same level of protection for whatever type of works are concerned. This twofold regime could lead to surprising consequences. For instance a technological tool could be apply to protect both software and audiovisual works. Its circumvention would

¹¹⁸⁹ See: Directive 91/250/CEE, JO L 122/42, 17.05.91.

be unlawful when applied to audiovisual works, but would not be when applied to software.

An encryption key could be used to encrypt both computer programs and films. One person would post the decryption key on the Internet, without pursuing any commercial purpose. She could be sued under the transposition of the 2001 directive, that does cover commercial and non commercial activities of trafficking in circumvention devices, but not under the earlier directive as far as computer programs are concerned. In practice that would exclude the copyright holders in the software using this particular encryption from the possibility to bring an action against her.

It has been said that no modification of the *acquis communautaire* was required since the main features of article 6 of the directive on the copyright in the information society were already reflected in the software directive¹¹⁹⁰. The software industry has also alleged that the regime of the former directive was functioning well in practice. If so, we could wonder why the extended protection envisaged in the new directive, including the act of circumvention and any non commercial trafficking in circumventing devices, would be better adapted than a more restricted regime that proved to be adequate. It is worthwhile to note that if the protection against circumvention of software is not regulated under the article 6 of the 2001 directive, it implies that the software industry is not obliged to take measures to accommodate some exceptions. This likely satisfies the software industry.

VI Conclusion

The legal protection against circumvention granted by the European directive of the 22d of May, 2001, is likely the most extensive protection in all implementations of the WIPO Treaties of 1996. It covers a whole range of technological measures, from anti-copy devices, monitoring and tracking systems, digital rights management to access controls; it protects the technical conveyance of the exclusive rights, as well as of any use of the work that would not be authorized by the copyright or related right holders, even beyond the scope of the copyright monopoly; it prohibits both the circumvention and the trafficking in devices that could enable or facilitate it. Neither the United States, nor Australia, nor Japan, have been that far.

As far as the issue of the copyright exceptions is concerned, the European legislator has been rather audacious. Instead of exempting circumvention activities where carried out in the purpose of a legitimate use, it tries to impose the exercise of some exceptions to the operation of technological measures. This implies that the exceptions are given a positive meaning and not only a defensive nature. It is certainly the first time that authors are asked to facilitate the exercise of exceptions to their rights.

¹¹⁹⁰ See: Reinbothe (2001): 80/5.

Having said that, the boldness of the directive is constrained by a number of features. Only some exceptions are concerned and the initiative mainly lies upon the rightholders. The exception to the copyright becomes a matter for negotiation and contracting, in favor of the authors. The legislative power has yet to intervene but only subsidiarily to the measures taken by the authors.

More essentially, the general exemption granted in favor of on demand services, hence in favor of most of the business models that will govern the distribution of works on the Internet, will likely to jeopardize the fragile balance the article 6(4) seeks to achieve. At the end of the day, it surely appears that this balance is strongly tipped in favor of the copyright and related right holders who, despite their strong opposition to this odd provision, might not be so disadvantaged thereby than they pretend to be.

4.3 Protection of Digital Content and DRM Technologies in German Copyright

4.3.1 The German Copyright — Yesterday, Today, Tomorrow

*Thomas Dreier, Georg Nolte*¹¹⁹¹

Today, due to the challenges brought forth by digital and networked information technologies, we see a “crisis” of the finely tuned copyright system as we know it. Internationally, we are in the midst of adjusting the copyright system to its future tasks. Within the next weeks the EU-Directive on Copyright in the Information Society will be implemented into the German Copyright Law. However, still many issues remain unresolved. The proper scope of the exception clauses as laid down in §§ 45 et seqs. of the German Copyright Act and, in particular, the private use exception of § 53, is still subject to discussion. This question interrelates with the upcoming implementation of technological protection measures (TPM) and digital rights management systems (DRM). For now, the legislature has granted strong legal protection for TPM that might eventually undermine the underlying values of the statutory exception clauses. A look back to the initial rationals of our copyright system might help to find a proper balance of interests for the future.

I Introduction

Copyright has been called the “Magna Charta” of the information society.¹¹⁹² While some commentators have prophesied that, in view of digital information technology, copyright will become obsolete¹¹⁹³, today it seems more likely that copyright will see a strengthening of its traditional role for the development of culture. Moreover, in all likelihood, copyright will assume the role of a steering instrument with regard to the regulation of the way, in which information is produced, made accessible, distributed and, ultimately, consumed, in our society. However, both the advent of digital information technologies and mounting criticism of the “proprietary”, exclusionary nature of copyright have led to a true “copyright crisis”. At present, we find ourselves in the midst of the search for a proper structure and scope of a future copyright that will fit to the needs of the evolving information society, both at the national and the international level.

The history of copyright can be understood as the consecutive reaction to the social and economic changes brought about by new technologies. The copyright system as we know it today come into being as a reaction to the then modern technology of Gutenberg’s printing press. Later new technologie arrived,

¹¹⁹¹ University of Karlsruhe

¹¹⁹² See: Hoeren (2000): 3.

¹¹⁹³ See: Negroponte (1995): 58. Barlow (1996): 169, 174. Saniers (2000): 379, 397.

which revolutionized the storage and reproduction of works (photography, phonorecords, magnetic tapes, copy machines, and, finally, digital storage media) as well as their dissemination (radio, television, and, finally, the Internet). This provoked several consequences. First, works became easier to copy. Second, production of such copies increasingly shifted from the producers to the end-users. Third, the overall number of copyright relevant transactions has dramatically increased over the last decades. Most copyrighted works are now mass-produced. Fourth, this resulted in a shift of the rationale of copyright from a cultural to an industrial right.¹¹⁹⁴ In addition, to the same extent copyright became subject to economic desires. Correspondingly, the technological developments and corresponding changes regarding the subject matter protected by copyright law have led to discrepancies with regard to its initial protective purpose.¹¹⁹⁵ Whereas at the beginning of copyright in the 18th century the main focus was on the philosophical attribution of the work to its ‘spiritual father’ and the personal interests of the author, today the economic implications of copyright in the frame of the ‘copyright industries’ are likewise at stake.¹¹⁹⁶ Securing the individual author’s alimentation is only one part of copyright. Increasingly, amortization of the producers’ investments is the other. Hence, like any other intellectual property right, copyright becomes a battlefield for the fight for market share.¹¹⁹⁷

But the tasks attributed to copyright don’t stop there. In the digital and networked information society, copyright has to regulate the conditions of how information products are being created, disseminated and consumed, and how users have access to works and underlying ideas. Since this task is much broader than the area of copyright — indeed it is the area of law increasingly referred to as “information law” — the current “crisis” of copyright may be explained by the fact that copyright as a body of law is currently overloaded with information policy issues, which — like a ship carrying a too heavy load — it has never been designed for.

The balance between the interests of authors and other rights holders and the interests of the general public has traditionally been achieved by granting to the author strong exclusive rights that are protected by the guarantee of property laid down in Art. 14 German Constitution, on the one hand, and subjecting them to certain limits and exceptions on the other. If the exclusive rights granted to the authors conflict with legitimate interests of users and the general public, the law limits the exclusive rights so that protected works may be used without the permission of the author in some situations even without compensation. Public interests which justify such limitations and exceptions are the freedom of information and the freedom of intellectual creation, as well as considerations of market failure, i.e. cases in which individual transactions either fail or require unreasonably high transaction costs, and where the law remedies this situation

¹¹⁹⁴ See: Schricker (1992): 242.

¹¹⁹⁵ See: Wandtke (2002): 11.

¹¹⁹⁶ For a critical view, see: Dietz (1988): 200, 202.

¹¹⁹⁷ For discussion of the legal implications of copyright serving as an instrument for allocating markets, see: Dreier (2001): 51.

by granting the authors a claim for remuneration. Over decades copyright has thus evolved into a finely tuned system that balances the rights of authors and other rightsholders and the interests of the public.

However, the existing limitations as laid down in §§ 45 et seq. of the German Copyright Act need to be revised, because they have been crafted against the background of analog reproduction technologies.¹¹⁹⁸ Due to the ease, low cost, speed and high quality of digital copies, these interests are no longer the same in the digital context as they were in the analog context. In all likelihood, a literal application of existing private copying rules would be too far-reaching in the digital context. Furthermore, the advent of technological protection measures (TPM) and digital rights management systems (DRM) may lead to a situation where this market failure no longer exists. The situation is further complicated by the fact that, at least at present, it is but clear how successful TPM/DRM will become in the future, and whether or not — and if so to what extent — TPM/DRM will be accepted by users and end-users. What is clear, however, is the fact that once the legislature has decided that TPM/DRM should be applied to copyright, then the issue of how far the legal protection of TPM/DRM against illegal circumvention should reach has to be addressed.

With the Copyright Amendment of 2003,¹¹⁹⁹ which implements the EU-Directive on Copyright in the Information Society¹²⁰⁰ into national law, the German legislature will take a first — still somewhat insecure — step to adjust copyright to the challenges set by digital and networked technology. Before the present German solutions will be discussed, (III.), a brief overview of German Copyright history will be given (II.). A brief outlook concludes this chapter (IV.).

II The Past

II.1 The Origins of German Copyright

From a historical perspective, copyright is a rather young legal concept. Neither ancient Greek nor ancient Rome granted a legal protection for creative acts. Artistic works were not understood as individual acts of creation but as mere imitations of an unchanging idea of beauty or of the work of God. Later, the invention of the printing press led to mass production of literary works, and — contrary to the earlier monks' activity of manually copying books, which did not result in a tremendous output of copies — the printing press permitted a substantive number of relatively cheap reprints. This, however, had the effect

¹¹⁹⁸ See: Dreier (1997): 139.

¹¹⁹⁹ The passing of the "Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft" is expected in July 2003, after few last matters of dispute are settled by the mediation committee of Bundesrat and Bundestag.

¹²⁰⁰ Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ EU. No. L 167 of 22.6.2001, p. 10.

of satisfying a market demand — as modern economists would say — which the initial publisher would have needed to satisfy in order to make good on his initial investment. Hence, to secure the production of original editions, a legal remedy was needed to suppress the unauthorized reprint of books. True, in the 16th and 17th century so-called “print-privileges”, justified by the initial investment, were granted to the publisher, but in Germany the privileges could only provide a limited protection due to the highly fragmented German territorial landscape. Therefore, at a time when natural law flourished in Europe, lawyers and philosophers searched for a theoretical concept that would provide a universal foundation for the unlawfulness of reprints.¹²⁰¹ The act of creation by the author was seen as the source of a right for his works. From this initial right of the author the legitimacy of the publisher’s action against reprinters could be deduced. During the 18th century the foundation of the right of the author as a natural right evolved into the theory of intellectual property. The theory of *John Locke* on property, according to which the work of man was the base for property, could be transferred to intellectual works. Moreover the personality of the author, his spiritual relation to his creation, was seen as a source of copyright. Thus, in the German tradition copyright was understood as a moral right rather than a mere exploitation right.¹²⁰²

Quite like the continental “droit d’auteur” tradition, the approach taken by the German “Urheberrecht” constitutes a fundamental difference to the Anglo-American copyright system. Contrary to the Anglo-American tradition with its strong utilitarian approach, the continental copyright system is still much more focused on the person of the creator. The droit d’auteur as such is inalienable.¹²⁰³ Thus a doctrine like “works made for hire” could not exist in German copyright. Moreover, a legal entity cannot be the initial owner of copyright, but only the owner of a so-called neighboring right (“verwandtes Schutzrecht”). Of course the German copyright allows the transfer of exploitation rights, however copyrights have the tendency to remain as far as possible with the original author.¹²⁰⁴ In cases of doubt it is assumed that only those rights have been transferred that are necessary in view of the purpose of the initial transfer.¹²⁰⁵ Also the transfer does not include methods of use that were unknown at the time of the transfer.¹²⁰⁶ Furthermore, after the amendment of the German copyright contract law in 2002, authors are by law entitled to receive a “reasonable” remuneration for the transfer of their exploitation rights.¹²⁰⁷

¹²⁰¹ See: Kant (1987): 137. Fichte (1987): 155.

¹²⁰² It should be noted, however, that due to its foundations in natural law, copyright has not been designated as ‘intellectual property’, a term reserved to tangible property; See: Kohler (1880): 155. Dölemeyer, Klippel (1991): 185, 223, 227.

¹²⁰³ § 29 (1) of the German Copyright Act.

¹²⁰⁴ See: Ulmer (1980): 292.

¹²⁰⁵ § 31 (5) of the German Copyright Act.

¹²⁰⁶ § 31 (4) of the German Copyright Act.

¹²⁰⁷ § 32 (1) of the German Copyright Act.

II.2 The German Copyright Act of 1965

This is not the place to retrace the whole German copyright history with its laws of 1876 and, most notably, those of 1901 and 1907.¹²⁰⁸ Suffice it to say that the adoption of the Copyright Act¹²⁰⁹ in 1965, still in force today, was a milestone in the history of German copyright law, summing up half a century of case law and reacting to what was then the most advanced reproduction technology.¹²¹⁰ The purpose of the new Copyright Act was to strengthen the rights of authors and other rights holders. The scope of the copyright exceptions were partially reduced and the term of protection extended to 70 years *post mortem auctoris*.¹²¹¹

In the center of the discussion was the future scope of the private use exception in view of the enlarged copying facilities opened up by both the magnetic tape recorder and reprography machines. In particular, the music industries feared that the home taping of music from the radio would infringe upon the primary market of phonorecords,¹²¹² and publishers feared a decrease in sales of their printed books and periodicals by the advent of copy machines. However, there was general agreement that the exception for private use should remain in principle.¹²¹³ The issue debated was to what extent new methods of mechanical reproduction should fall under this exception, a question which was to a large extent influenced by prior case law of the German Federal Supreme Court (Bundesgerichtshof; BGH). Thus, in 1955 the Federal Supreme Court had decided that photomechanical reproductions of scientific articles for internal company uses were an infringement of copyright.¹²¹⁴ The consequence of this decision had been that a framework agreement was concluded by authors and the industry regarding a levy for the making of those copies for in-house uses.¹²¹⁵ Also, the question, whether copies made on magnetic tapes should be embraced by the private use exception had already been the subject of several decisions of the Federal Supreme Court.¹²¹⁶ In a first case, the Court decided this conflict of interest in favor of the rights holder by excluding magnetic tape recordings from

¹²⁰⁸ The “Gesetz betreffend das Urheberrecht an Werken der Literatur und der Tonkunst” (1901) and the “Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie” (1907).

¹²⁰⁹ Gesetz über Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz).

¹²¹⁰ For preparatory work and discussion see: Ulmer (1965): 18.

¹²¹¹ For summarizing overviews see: Ulmer (1965): 18. Fromm (1965): 50. Samson (1966): 1.

¹²¹² Due to their very high price video recorder were not very disseminated at these times.

¹²¹³ According provisions were laid down in § 15 (2) LUG and § 18 KUG.

¹²¹⁴ BGH, June 24th 1955 (Fotomechanische Vervielfältigung), BGHZ 18, 44 = UFITA Vol. 20 (1955), 346.

¹²¹⁵ Contracting parties were the Bundesverband der Deutschen Industrie and the Börsenverein des Deutschen Buchhandels.

¹²¹⁶ BGH, May 18th 1955 (Grundig-Reporter), BGHZ 17, 266 = GRUR 1955, 492 = NJW 1955, 1276 = UFITA Vol. 20 (1955), 314; BGH, January 22nd 1960 (Werbung für Tonbandgeräte), GRUR 1960, 340 = UFITA Vol. 31 (1960), 335; BGH, June 12th 1963 (Tonbänderwerbung), GRUR 1964, 91 = UFITA Vol. 40

the private use exception, since in its view recording on magnetic tape could compete with the commercial sale of the protected works in question, and was therefore not covered by the value judgment underlying the private use exception.¹²¹⁷ Of course, the reproductions that took place within the private sphere could not be controlled,¹²¹⁸ and only few owners of a tape recorder did pay the annual fee asked for by collecting societies. In another decision of 1964, the Federal Supreme Court regarded the producers of tape recorders as being responsible for the later use of their recording devices to make recordings from copyright protected works, and hence subjected them to the payment of remuneration to the rights holders.¹²¹⁹ The shifting of the claim for remuneration against the end-user to claim of remuneration against the producer was considered justified since the producers indirectly profited from the fact that their devices could be used to reproduce copyrighted material.¹²²⁰ Moreover, the producers could pass on the additional costs to the end-user. With this constructive solution the jurisdiction had broken new grounds in copyright. It was taken over by the legislator of the Copyright Act of 1965 and found its way into the newly formulated private use exception.

According to § 53 of the German Copyright Act (1965) it was to a certain extent permitted to make copies of copyrighted works for personal use without the permission of the rights holder, initially even without owing remuneration for this use. The exception went so far as to allow the reproduction of complete books, since at that time reprography was still rather expensive so that it was not feared to seriously affect the sales of books.¹²²¹ Later, the courts limited the number of copies to be made under this provision to seven.¹²²² To the contrary, for reproductions made on video or audio recording media, the author was granted a claim for remuneration against the producer or the importer of recording devices.¹²²³ This claim was limited to 5 % of the selling price and had to be asserted by a collecting society. Similarly, § 54 of the German Copyright Act permitted the making of copies for certain non-personal uses (e.g. for scientific purposes).¹²²⁴ For other non-personal purposes copies were only allowed if minor parts of works or single articles published in newspapers or magazines were affected or if the work had been out of print for more than two years. However, if such a reproduction was used for commercial purposes, a reasonable

(1963), 362; BGH, June 19th 1963 (Werbung der Tonbandgeräthändler), GRUR 1964, 94 = UFITA Vol. 40 (1963), 371; BGH, May 29th 1964 (Personalausweise), GRUR 1965, 104 = UFITA Vol. 43 (1964), 134.

¹²¹⁷ BGH, May 18th 1955 (Grundig-Reporter), BGHZ 17, 266.

¹²¹⁸ See: Ulmer (1965): 18, 32.

¹²¹⁹ BGH, May 29th 1964 (Personalausweise), GRUR 1965, 104. — If the rights holders would make use of this claim for remuneration against the producer, they had, however, to be satisfied by a once time lump-sum payment.

¹²²⁰ See: BGH, May 29th 1964 (Personalausweise), GRUR 1965, 104.

¹²²¹ See: Ulmer (1965): 18, 31.

¹²²² BGH, April 14th 1978 (Vervielfältigungsstücke), GRUR 1978, 474, 476.

¹²²³ See § 53 (5) of the German Copyright Act (1965).

¹²²⁴ For details see the exact wording of § 54 of the German Copyright Act (1965).

remuneration had to be paid to the rights holders.¹²²⁵ § 53 (5) and § 54 (2) of the German Copyright Act (1965) were statutory licenses, which reduce the exclusive right to a mere claim for remuneration. The philosophy behind this legislative approach, which was intended to serve as a model for future reproduction technologies,¹²²⁶ is well expressed in the German saying that “it is better to have a small bird in your hand than a big bird on your roof”, i.e., a claim for remuneration is better than an exclusive right which in practice cannot be enforced.

With regard to its importance on the information society, a particular mention should be made of the additional statutory license introduced by § 49 (1) of the German Copyright Act for the reproduction of news-articles, if these were used in other newspapers or similar publications.¹²²⁷ Here also, the authors were granted a claim for remuneration. Other exceptions concerned the use of copyrighted works for the administration of justice and public safety;¹²²⁸ collections for religious, school and institutional use;¹²²⁹ for school broadcasts;¹²³⁰ of public speeches;¹²³¹ visual and sound reporting;¹²³² quotations;¹²³³ a limited array of public communications;¹²³⁴ ephemeral recordings by broadcasting organizations;¹²³⁵ reproductions and public communication by certain commercial enterprises;¹²³⁶ works incidentally reproduced or publicly communicated;¹²³⁷ catalog illustrations;¹²³⁸ works in public places;¹²³⁹ and, finally, portraits.¹²⁴⁰

II.3 The Copyright Amendment of 1985

Already a decade after the entering into force of the Copyright Act of 1965 it became apparent that the development of reproduction technologies had resulted

¹²²⁵ § 54 (2) of the German Copyright Act (1965).

¹²²⁶ See the explanatory memorandum to the draft Act, UFITA Vol. 45 (1965), 240, 245.

¹²²⁷ For details see § 49 of the German Copyright Act. According to the prevailing opinion this provision allowed the use of articles in press-reviews and press-clippings.

¹²²⁸ § 45 of the German Copyright Act.

¹²²⁹ § 46 of the German Copyright Act. — It should be noted that the initial royalty free use was declared unconstitutional by the German Constitutional Court, and subsequently replaced by a claim for remuneration; see BVerfGE 31, 229 = GRUR 1972, 481 = NJW 1971, 2163.

¹²³⁰ § 47 of the German Copyright Act.

¹²³¹ § 48 of the German Copyright Act.

¹²³² § 50 of the German Copyright Act.

¹²³³ § 51 of the German Copyright Act.

¹²³⁴ § 52 of the German Copyright Act.

¹²³⁵ § 55 of the German Copyright Act.

¹²³⁶ § 56 of the German Copyright Act.

¹²³⁷ § 57 of the German Copyright Act.

¹²³⁸ § 58 of the German Copyright Act.

¹²³⁹ § 59 of the German Copyright Act.

¹²⁴⁰ § 60 of the German Copyright Act.

in a drastic increase in the reproductions made of copyrighted works for personal and non-personal use, and that the Copyright Act had to be adjusted. After several years of discussion, in 1985 the legislature reacted to these technological changes and the further shift of reproduction processes into the private sphere by limiting the number of acts which could be undertaken even without payment of some sort of remuneration, and by expanding the successful system of lump-sum levies introduced in 1965.¹²⁴¹ First, the remuneration claim against the producer of devices for the reproduction of musical works and (audio-) visual works was upheld. Second, for video and audio recording media, an additional claim for reasonable remuneration was introduced against the producer of blank sound- or videotapes.¹²⁴² Third, according to a newly implemented § 54 (2) of the German Copyright Act (1985)¹²⁴³ a lump sum payment is to be made by the producer or importer of photocopiers. And, fourth, a reasonable remuneration claim was granted against persons (or institutions) who operate copy-machines on a large scale.¹²⁴⁴ According to § 54 (4) German Copyright Act (1985)¹²⁴⁵ an appendix to the copyright Act stipulates what was considered to be a reasonable remuneration.¹²⁴⁶

With the Amendment of 1985 Germany had been the first country that had introduced a complete system of remuneration regarding the reproduction of musical works, (audio-) visual works and literary works for personal and certain cases of non-personal uses. This system allowed the end-user to benefit from the new technologies by making private copies of protected works without the prior permission of the rights holder, and to have uncomplicated and open access to cultural and informational goods, while safeguarding the (monetary) interests of the rights holder as guaranteed by Art. 14 of the German Constitution. Since the reproduction acts made for private or other personal uses were not individually registered, the privacy of the end-users was also safeguarded. Consequently, collecting societies played a major role in this field, since they are the only organizations entrusted by law to collect the remuneration. This supports strong rights holders' organizations, but it also benefits those who have to pay the remuneration since it presents them with a "one-stop-shop".

It should be noted that when legal protection of computer programs was for the first time introduced into the German Copyright also in 1985,¹²⁴⁷ the legislator

¹²⁴¹ Regarding the Amendment of 1985 see: Möller (1986). Hillig (1986): 11. Dietz (1985): 15.

¹²⁴² § 54 (1) of the German Copyright Act.

¹²⁴³ Today: § 54a (1) of the German Copyright Act.

¹²⁴⁴ § 54 (2) of the German Copyright Act (1985); today: § 54h of the German Copyright Act.

¹²⁴⁵ Today: § 54d (1) of the German Copyright Act.

¹²⁴⁶ Those lump-sum levies (which haven't changed ever since) are, however, rather low; see: Nordemann (1985): 837, 840. Schack (2002): 497, 499.

¹²⁴⁷ By way of inclusion in the list of protected works in § 2 (1) no. 1 of the German Copyright Act. – Prior to this clarification the jurisdiction and legal literature had already assumed software programs as protected by copyright, see: Ulmer (1971). But the German Courts had required a rather high level of originality

completely excluded the private copying-exception for computer programs in view of the ease of copying and the threat that unauthorized copies might have on the primary market. This complete ban of private copies was later eased in the course of the implementation of the EU-Directive on the legal protection of computer programs,¹²⁴⁸ which introduced a specifically designed set of limitations into German Copyright Law.¹²⁴⁹ Similarly, after the EU harmonized the legal protection of databases,¹²⁵⁰ the private use exception was abolished for database works and a special set of limitations regarding the new sui-generis right was introduced into the German Copyright Act.¹²⁵¹

III The Present

III.1 The Digital Dilemma

The advent of digital technologies however, poses a fundamental challenge to this finely tuned system that had evolved to balance the interests in times of analog technologies. The digital format has revolutionized the production and the exploitation of works far more than any other technological achievement since Gutenberg's printing press. Digital technology has not only brought forth new types of works and changed the ways in which works are created and distributed. Also it enables the making of copies of perfect quality, at no time and at — almost — zero marginal cost. In addition, at least in theory, it only needs one such copy to be stored on any one server accessible via the Internet in order to satisfy the worldwide demand for any particular copyrighted work. This has led to a further shift of reproductions activities from the producer's side to the end user's side. Today in almost every household one can find a PC that is connected to the Internet and devices that enable to make copies of copyrighted works (e.g. printer or CD-burner). Thus the Internet has been described as a "*giant, out of control copying machine*".¹²⁵² In economic terms, these technologies dramatically increase the possibilities for piracy and therefore tend to severely imperil the investment made in original copyrighted material, and erode the very purpose of the copyright system itself that is to grant legal protection to immaterial goods in order to secure their production, dissemination and use.

It comes as no surprise that the economic changes brought about by digital and networking technologies make authors and rights holders ask the legislator for stronger legal copyright protection. In addition, rights holders increasingly

for computer programs in order to enjoy copyright protection; see BGH, May 9th 1985 (Inkasso-Programm), GRUR 1985, 1041, 1047.

¹²⁴⁸ Council Directive of 14 May 1991 on the legal protection of computer programs (91/250/EEC), OJ EU, No. L 122 of 17.5.1991, 42.

¹²⁴⁹ §§ 69c-e of the German Copyright Act.

¹²⁵⁰ Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ EU No. L 77 of 27.3.1996, 20.

¹²⁵¹ §§ 55a and 87c of the German Copyright Act, introduced by Art. 7 of the Information and Communication Services Act of 22.7.1997, German OJ, 1997-I, 1870.

¹²⁵² See: Shapiro, Varian (2001): 83.

use technical safeguards in order to control both access to, and further use of, copyrighted material in digital form. Since any such technical protection measure is itself vulnerable to technical circumvention, additional legal protection is claimed against the unauthorized circumvention of such technical protection measures. On the other hand, we find the interests of users, open source adepts, second sourcers and providers of information value-added products and services. Together with information theorists these groups fear, that in the digital and networking context copyright, already as it presently exists, monopolizes too much of the public domain, not to speak of the further diminishing of the commons when it comes to increasing copyright protection. From this point of view, copyright is seen as limiting free speech, a threat to the free exchange of ideas, a hindrance to innovation and, finally, responsible for reducing public welfare. While providers of information-value-added products and services claim that copyright reserves too many secondary markets, thus concentrating market power and eliminating competition, users tend to think that a law which criminalizes a large part of the population without being properly enforced doesn't make sense. Its not just that users want to make digital copies of works they have purchased as they were able to in the analog environment, they also want to take part in the creative process by remixing culture from the past. Digital technology enables everybody to produce new works, which are based on pre-existing material. "Rip, mix, burn" as an Apple commercial suggests.¹²⁵³ The effects of this change for the future production of culture are so far little understood.

At present, it seems that internationally the reactions of legislators tend to concentrate mainly on the concerns of the rights holders and their fear of loss of control. Moreover, a danger is perceived that TPM/DRM-systems and an overly broad acceptance of the validity of standard clauses in the online environment will lead to private legislation that quite like TPM might override legislative copyright exceptions. As regards the copyright exceptions, in particular representatives of the copyright-industries argue that private use exceptions such as laid down in §§ 53, 54 of the German Copyright Act have been merely a reaction to the market-failure that reproductions in the private sphere could not be controlled or at least would lead to disproportionate high transaction costs. It is then concluded that the private use exception will lose its justification due to DRM-systems that could rectify this market failure.

However, this view tends to overlook the overriding considerations that have led to the fundamental decision of the legislator which are expressed in §§ 53, 54 German Copyright Act. As the German legislative history has demonstrated, the private use exception is only partly based on market failure. In addition, the legislature of 1965 intended to react to what had become a general understanding, namely that the private sphere should be kept free from copyright claims. The legislator did not want to give in to a practice of abusing copyright, but meant to bring the law in line with this understanding of the general public.¹²⁵⁴ In

¹²⁵³ See: Lessig (2001a): 188.

¹²⁵⁴ See the explanatory memorandum to the draft Act, UFITA Vol. 45 (1965), 240, 245 and 289.

adopting the system of claims for remuneration, the legislator made clear that reproductions within the private sphere remain in principle subject to copyright. However the exclusive right of the author was reduced to a remuneration claim. The main interests of the authors was not seen in being able to prohibit certain uses, but to be granted a reasonable award for such uses. Similarly, with the exemption of non-personal uses, the legislator reacted to what had become a practice in business and science. In this respect, the explanatory memorandum of the Draft Act expressly states that a hindrance to the free flow of information in business and science should be avoided. In particular, the work of scientists should not be hindered by the obligation to get a prior permission of the rights holder in order to make copies of protected works.¹²⁵⁵ In sum, the provisions of §§ 53, 54 German Copyright Act have to be understood as doing more than just correcting market failure. Rather, these provisions were intended to serve legitimate interests of the general public, e.g. to have open access to cultural goods or privacy.¹²⁵⁶

III.2 Case Law Regarding the Application of the Exception Clauses in the Digital and Networked Environment

In recent years, prior to the implementation of the EU-Directive on Copyright in the Information Society, the German Federal Supreme Court had to decide at several instances to what extent the traditional exception clauses also apply in cases where modern information technology leads to a higher use intensity of copyrighted subject matter. The issue common to all these cases decided was to find out whether or not third parties could provide value-added information products and services that are based on pre-existing copyright protected material without permission of the holders of rights in the original material. The Federal Supreme Court chose as a starting point the supposed rule according to which exceptions to the exclusive rights are subject to a narrow interpretation. Somewhat reluctant at first, the Court later on indeed allowed some of these value-added information services and provided some guidelines as to their possible limits. Although not all of these decisions had to deal with digital technology, they nevertheless all shed light on the on the issue. Following, these cases shall briefly be discussed.

Still concerning an information service in the analog environment, the Federal Supreme Court ruled in 1997 that an information service provider is not allowed to make copies of archived articles and deliver them to its customers, if this service is bundled with a prior research service.¹²⁵⁷ The Court argued that the combination of making copies (which is as such permitted by § 53 of the German Copyright Act) with a prior research service (which as such is not subject to copyright) would exceed the limits of the private use exception as ini-

¹²⁵⁵ See the explanatory memorandum to the draft Act, op.cit., at 288, 289.

¹²⁵⁶ See the explanatory memorandum to the draft Act, op. cit., at 240, 278.

¹²⁵⁷ BGH, January 16th 1997 (CB-Infobank I), GRUR 1997, 459; BGH January 16th 1997 (CB-Infobank II), GRUR 1997, 464.

tially intended by the legislature. In 1998, the Federal Supreme Court ruled that § 53 (2) no. 2 of the German Copyright Act (according to which copies can be made for archival purposes) does not apply to digital copies made in order to build up an electronic archive.¹²⁵⁸ Again, the Court referred to the intention of the legislature in 1965,¹²⁵⁹ according to which § 53 (2) no. 2 of the German Copyright Act was only intended for very limited purposes.¹²⁶⁰

However, two later decisions of the Federal Supreme Court seem to indicate a somewhat modified view of value-added services and the application of the exception clauses on uses that are based on modern technologies. The first of these two decisions concerned the making of copies and their delivery by public libraries.¹²⁶¹ The problem is that the private use exception in principle allows that private copies can be made by a third party. However, in a digital environment this might lead to an intensity of use that by far exceeds what the legislature had intended to be exempt from copyright some 40 years ago. Libraries can make their catalogues available online and send the copies with no loss of time via fax or e-mail to their users. In spite of this, the Federal Supreme Court, by referring to the overriding significance for the general public to have an open access to relevant information, held that such a copy and delivery service by public libraries is still covered by the private use exception. However, in order to compensate rights holders for the higher intensity of use, and also in order to comply with the “three-step-test” contained in artt. 13 TRIPS and 9 (2) of the Berne Convention, the Federal Supreme Court ruled that the rights holders are entitled to an additional compensation.¹²⁶² This seems to be a wise decision, indeed: It provides that the public has an easy access to relevant information while at the same time safeguarding the monetary interests of the rights holders.¹²⁶³ The second decision followed in 2002,¹²⁶⁴ which might have far reaching implications on future decisions regarding value-added products and services. Here, the issue was whether press-clippings in digital formats are at all, and if so, to what extent privileged by the provision of § 49 of the German Copyright Act, which allows press reviews against payment of an adequate remuneration.¹²⁶⁵ Referring

¹²⁵⁸ BGH, December 10th 1998 (Elektronische Pressearchive), GRUR 1999, 324.

¹²⁵⁹ See the explanatory memorandum of the draft Act, *op. cit.*, at 289.

¹²⁶⁰ E.g. securing the stock of works or space-saving storage.

¹²⁶¹ BGH, February 25th 1999 (Kopienversanddienst), GRUR 1999, 707.

¹²⁶² Following this decision public libraries and the collecting societies concluded a framework agreement on lump-sum payments that differ depending on whether the copies are demanded for private, scientific or commercial uses.

¹²⁶³ It has to be noted, however, that this ruling does not include a situation where libraries build up electronic archives to supply the demand of those copies. For each single request they have to make an individual copy.

¹²⁶⁴ BGH, July 11th 2002 (Elektronischer Pressespiegel), GRUR 2002, 963.

¹²⁶⁵ § 49 of the German Copyright Act provides — at least according to the prevailing opinion in legal literature — that newspaper articles may be used for press-reviews and press-clippings without getting a prior permission by the publisher. Digital press-clippings, however, are easy to make and can be delivered online to millions of users without any loss of time and at almost zero

to the principle of a narrow interpretation of copyright exemptions, the lower courts had — in accordance with the prevailing opinion in legal literature — denied to apply § 49 German Copyright Act to digital press-clippings, even if such press-clippings were produced only for inhouse-use. The Federal Supreme Court, however, found a reasonable compromise: Firstly the Court argued that the format used — digital or analog — is as such irrelevant when it comes to decide whether or not a pressclipping service is privileged by the exception clause of § 49 German Copyright Act. Second, the Court held that if the digital format leads to a completely new way of use, a different legal treatment is justified. In the case to be decided, which only concerned press-clippings made for inhouse-use, the Federal Supreme Court held that digital press-clippings are in principle permitted, but only if they are produced in graphic (read-only) files that do not allow keyword-search and therefore cannot be used to build up electronic archives of the articles contained in the press-clippings. The Court did not have to decide on press-clippings offered to the general public, but it may be concluded from the reasoning of the Court that electronic press-clipping services which are not limited to inhouse-use, would go beyond what is allowed by the exception contained in Sec. 49 of the German Copyright Act.

III.3 The Copyright Amendment Act of 2003

Today, answers to the technological developments can no longer be confined to nation states. The adjustment of copyright in a networked environment has become a global concern. In 1996, the World Intellectual Property Organization (WIPO) has passed two treaties, the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty (WPPT). Main features of these treaties are the introduction of a new making available right and the legal protection of technical protection measures (TPM) on an international level. In 1998, the USA has passed the Digital Millennium Copyright Act (DMCA) to bring their national law in accordance with the WIPO-Treaties. In June 2001 the EU passed the Directive on Copyright in the Information Society.¹²⁶⁶ The Directive does not only implement the obligations made by the WIPO-Treaties, but also harmonizes some core elements of copyright, especially the complex field of exceptions and limitations.

The Copyright Amendment Act of 2003¹²⁶⁷ aims both at implementation the EU-Directive into German law, but likewise to adjust German copyright to the context of digital and networked exploitation of works. The changes made do not only focus on the effective protection of rights holders, but seeks to provide

marginal costs. Therefore, electronic press-clippings could pose a major threat to the sales of newspapers.

¹²⁶⁶ Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ EU. No. L 167 of 22.6.2001, p. 10.

¹²⁶⁷ The passing of the “Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft” is expected in July 2003, after few last matters of dispute are settled by the mediation comitee of Bundesrat and Bundestag. — For the explanatory memorandum of the draft Act see BT-Drucks. 15/38 of 6.11.2002.

a reasonable legal framework also for users and those who exploit copyrighted works, allowing an efficient use of new technologies and promoting the further development of the information society.¹²⁶⁸ However, in view of the task to bring the copyright system in accordance with the needs of a future information society the present amendment can only be seen as a first step. This is all the more true since due to the federal elections in fall 2002, the German legislature has not been able to meet the deadline for implementing the Directive into national law. The following overview focuses on the core elements of the amendment, and is thus limited to the new right of making available to the public (a), the various exceptions and limitations on copyright (b) and the protection of TPM and rights-management information (c).

a) Making Available Right

In §§ 15 (2) no. 2, 19a of the German Copyright Act, the exclusive right of making available to the public will be incorporated as an example of the right to communicate to the public. The right of making available to the public embraces the exclusive right to make works available to the public, by wire or wireless means, in such a way that members of the public may access them from a place and at a time individually chosen to them.¹²⁶⁹ This new exclusive right and its explicit formulation provides legal certainty regarding the nature and the level of protection of acts of interactive on-demand transmission of copyright works and subject matter protected by related rights over networks. However, it should be noted that it is not yet clear to what extent the new right covers also push-services,¹²⁷⁰ and how services in between traditional broadcasting and making available, such as web casting and simulcasting,¹²⁷¹ will have to be treated in the future.

b) Limitations and Exceptions

In principle, the implementation of the limitations and exceptions laid down in Art. 5 of the Copyright Directive didn't constitute a major problem for the German legislator. First, 20 of the altogether 21 exceptions listed in the Directive are optional, and second, the German system of limitations is largely reflected in Art. 5 of the EU-Copyright Directive. Moreover the directive provides a "grandfather clause" according to which Member States can maintain exceptions of minor importance, provided, however that they only concern analog uses.¹²⁷² Consequently, all of the exceptions existing in prior German Copyright law can be maintained, and they only have to be limited in certain respects. In some instances, the legislature also opted to take advantage of the freedom granted to Member States and enlarged existing limitations.¹²⁷³ Finally, the im-

¹²⁶⁸ Explanatory memorandum, *op. cit.*, at 14.

¹²⁶⁹ § 19a of the German Copyright Act.

¹²⁷⁰ For discussion, see: Bechtold (1998): 18, 25. Leupold (1998): 99, 106. Leupold, Bräutigam, Pfeiffer (2000): 575, 595. Spindler (2002): 105, 108.

¹²⁷¹ For discussion see: Dreier (2002b): 73.

¹²⁷² Art. 5 (3) (o) of the EU-Copyright Directive.

plementation act creates two new exceptions, one for handicapped people¹²⁷⁴ and the other one regarding the making available of protected works for purposes of teaching and research¹²⁷⁵. It should be noted that the German legislature did not feel obliged to expressly implement the three-step-test contained in Arts. 13 TRIPS and 10 WCT, 16 (2) WPPT and reiterated in Art. 5 (5) of the Copyright Directive,¹²⁷⁶ based on the assumption that both the Revised Berne Convention and the TRIPS-Agreement already bind Germany.¹²⁷⁷

aa) Private Use and Lump-Sum Levies

In the slightly modified wording of § 53 (1) of the German Copyright Act, the legislature will now make clear that reproductions can be made by a natural person for private use and for ends that are neither directly nor indirectly commercial “on any medium”, a wording adopted from Art. 5 (2) (b) of the EU-Copyright Directive. Thus, no distinction is made with regard to the technology used, which means that digital copies for private uses are covered by the private use exception under German copyright law. It remains unclear, however, whether or not the private use-defense requires that the first copy from which the second copy is made for private use-purposes, be itself legal. While there is some reason to apply § 96 (2) of the German Copyright Act by way of analogy,¹²⁷⁸ most commentators claim that it doesn’t make sense to apply a law that in practice cannot be enforced.¹²⁷⁹ The Second Chamber of Parliament (Bundesrat) had required a clarification that the copy used must in itself be legal. This question is still matter of dispute and is now expected to be decided by the mediation committee of both chambers of parliament (Bundestag and Bundesrat).¹²⁸⁰ Also still matter

¹²⁷³ See Explanatory memorandum of the draft Implementation Act, op. cit. at 17.

In fact, the great majority of exceptions existing in German copyright law was affected by minor changes which can therefore not be listed here in all detail.

¹²⁷⁴ § 45a of the German Copyright Act.

¹²⁷⁵ § 52a of the German Copyright Act.

¹²⁷⁶ According to this three-step-test, Member States have to confine any limitations of or exceptions (1) to certain special cases that (2) do not conflict with a normal exploitation of the work and (3) do not unreasonably prejudice the legitimate interests of the author. For interpretation see: Bornkamm (2002): 29. Lucas (2001): 423. WTO-Panel-Report of 15th June 2000 (United States — § 110 (5) of the U.S. Copyright Act), WTO-Doc.: WT/DS 160/R. It has been argued that once Member States have confined limitations to certain special cases, such as the EU in its Art. 5 of the Copyright Directive, the three-step-test effectively is reduced to a two step-test; see: Dreier (2002a): 29. Bornkamm (2002): 29, 43.

¹²⁷⁷ Explanatory memorandum of the Draft Act, op. cit. at 15. For German case law already applying the three-step-test see: BGH, February 25th 1999 (Kopierversanddienst), GRUR 1999, 707 and BGH, July 11th 2002 (Elektronischer Pressespiegel), GRUR 2002, 963.

¹²⁷⁸ According to § 96 (2) of the German Copyright Act, unlawfully made broadcasts may not be fixed on video or audio recording mediums nor publicly communicated.

¹²⁷⁹ See: Kreutzer (2001): 193, 200 with further references. Spindler (2002a): 60, 61 et seq. Schack (2002a): 165, 170.

of dispute is the question, whether or not digital copies for personal uses can be made by a third person.

However, the exception for non-personal uses¹²⁸¹ has seen some restrictions regarding its sentences 2 and 3 with regard to digital copies. In essence, digital copies are permitted only for scientific and archival purposes.¹²⁸² Electronic archives, however, may not be used for any direct or indirect commercial ends.¹²⁸³ It should be noted that the Copyright Directive does allow an exception regarding the making available of works to individual members of the public by dedicated terminals on the premises e.g. of publicly accessible libraries, for the purpose of research or private study.¹²⁸⁴ However, the German legislature did not make use of this possibility.

Most importantly, the German system of lump sum levy payments has been maintained. The Copyright Directive has left it open to Member States to introduce or maintain such a levy system.¹²⁸⁵ For certain limitations of the reproduction right (reproductions on paper or any similar medium¹²⁸⁶ and for private use¹²⁸⁷) as well as for broadcasts made by social institutions,¹²⁸⁸ the EU-Copyright Directive provides for a mandatory payment of a fair compensation. As criteria for the assessment of the compensation the Directive mentions the possible harm to the rights holder, the degree of use of TPM and regarding the private use exception, whether digital or analogue reproductions are in question¹²⁸⁹. It should be noted, however, it is currently disputed between collecting societies and hardware manufacturers whether blank recordable digital storage media and equipment which is likely to be used to make digital copies of protected works under the private use exception of § 53 of the German Copyright Act are subject to a levy payment or not. The Federal Supreme Court has so far ruled that a lump sum levy is indeed due for reader printers¹²⁹⁰, fax machines¹²⁹¹ and scanners¹²⁹². Moreover, The Regional Court of Stuttgart has deemed that CD-burners are subject to a lump-sum levy,¹²⁹³ and the Arbitra-

¹²⁸⁰ See the comment of the Bundesrat on the Draft Act (BT-Drucks. 15/38, p. 37). However the Federal Government replied that such a restriction could not be enforced in practice. Moreover would it ignore the social reality and would undermine the authority and credibility of the legal system (BT-Drucks. 15/38, p. 39).

¹²⁸¹ § 53 (2) of the German Copyright Act.

¹²⁸² See: § 53 (2) sentence 1, nos. 2 and 3, and sentence 2, no. 3 of the German Copyright Act.

¹²⁸³ § 53 (2) sentence 2, no. 3 of the German Copyright Act.

¹²⁸⁴ See Art. 5 (3) (n) of the Copyright Directive.

¹²⁸⁵ Recitals 35, 36 and 38.

¹²⁸⁶ Art. 5 (2) (a) of the Copyright Directive.

¹²⁸⁷ Art. 5 (2) (b) of the Copyright Directive.

¹²⁸⁸ Art. 5 (2) (e) of the Copyright Directive.

¹²⁸⁹ Recitals 35 and 38.

¹²⁹⁰ BGH, January 28th 1993, BGHZ Vol. 121, 215.

¹²⁹¹ BGH, January 28th 1999, ZUM 1999, 649.

¹²⁹² BGH, July 5th 2001, CR 2002, 176.

¹²⁹³ LG Stuttgart, June 19th 2001, ZUM 2001, 614.

tion Board within the German Patent and Trademark Office has concluded that a levy will have to be paid for computer hard disks as well. It is to be expected that both of these cases will go up to the Federal Supreme Court, which might ultimately have to decide to what extent other component parts of a computer system, such as, e.g., printers, and other storage media, such as, e.g. recordable CD and DVD, are subject to the levy provisions. While it seems almost inevitable that these questions will have to be answered in the affirmative, it is much less clear to what extent the outcome will be affected if rights holders use technical protection measures. Even if § 53 does not constitute a “right” to make private copies¹²⁹⁴, it would after all be inconsistent if users had to pay a lump-sum levy even in cases where rights holders prevent the making of private copies by applying copy control mechanisms.

bb) Making Available for Teaching and Research

According to § 52a of the German Copyright Act it will be permitted to a limited extent to publicly make available protected works for the purpose of illustration for teaching or scientific research, provided that access is restricted to a clearly defined group of users. This article enlarges the already existing provisions in German copyright law, which allowed reproductions for scientific or educational purposes.¹²⁹⁵ In both cases a reasonable remuneration has to be paid to the rights holder.¹²⁹⁶ Like other claims for remuneration within the exceptions as laid down in §§ 45 et seq. of the German Copyright Act, this remunerating claim can only be asserted by a collecting society. Prior to the making available for the purpose of teaching, the rightholder has to be asked for permission.¹²⁹⁷

This provision has been the one most fiercely fought over during the implementation process. While the Ministries of Finance of the German Länder stated that they could not any solution which would require them to pay an additional remuneration, publishers — in particular those of school books and of STM-material — claimed that the exception was so broad that it would erode the basis for the production of the material in question altogether, and hence violate both the authors’ and the publishers’ constitutional guaranteed property right.¹²⁹⁸ It should be noted, however, that already the wording of the new exception suggests a very narrow interpretation. Moreover a narrow interpretation seems to be mandated by the EU-Copyright Directive, which prohibits the publicly making available of works by non-profit establishments, such as publicly accessible libraries or archives.¹²⁹⁹

cc) Exception for the Benefit of Handicapped People

¹²⁹⁴ See: v. Diemar (2002): 587. Winghardt (2002): 349, 359.

¹²⁹⁵ § 53 (2) sentence 1, no. 1 and (3) of the German Copyright Act.

¹²⁹⁶ § 52a (4) of the German Copyright Act.

¹²⁹⁷ § 52a (2) of the German Copyright Act.

¹²⁹⁸ Art. 14 of the German Constitution. — For details see: Schack (2003): 1, 6.

¹²⁹⁹ See: Art. 5 (3) (n) and (c), as well as Recital 40 of the Copyright Directive.

Finally, with § 45a of the German Copyright Act another new exception will be introduced for the benefit of handicapped people. According to this provision non-commercial reproductions of works and their dissemination are permitted, if otherwise access to the works in question is not possible for handicapped people. For example, the perception of works could be made possible for blind people by transferring the work to Braille.

c) Technical Protection Measures and Rights-Management Information

Not unexpectedly, the second most controversial part of the new Copyright Act were the rules on legal anticircumvention protection and the protection of rights management information, as they will be laid down in §§ 95a–c of the German Copyright Act. The criticism is only in part due to the approach taken by the German legislature, which decided to implement the confusingly complex provisions of Art. 6 of the Copyright Directive almost verbatim into German law. On the one hand, rights holders criticized that the German legislature already at this stage had enacted provisions which subject rights holders to severe administrative fines if they fail to provide circumvention means to those users who benefit from the limited number of exceptions but cannot make use of them because of technical protections measures. On the other hand, users in Germany were not at all content with the fact that according to Art. 6 (4) (4) of the Copyright Directive, technical protection measures override all exceptions provided for by the Copyright Act, in cases where the works technically protected have been made available online on a contractual basis. Indeed, during the parliamentary debate, the representatives of the Green party suggested that implementation of the Directive should be stayed and the Directive be “handed back” to Brussels for appropriate amendment.

In order to better understand the legislative problem of legal protection against the making and use of anticircumvention devices, the problem shall be briefly recalled. In view of a never-ending race between new TPM and means to circumvent them, TPM are in need of string legal protection against their circumvention. In theory, any protection device can always be hacked. In practice, however, what is decisive is how easily and at what cost circumvention technology is available to the group of end-users for which a certain product is intended. In this regard the efficiency of legal protection granted to TPM should not be underestimated. Furthermore, once applied TPM cannot distinguish whether a certain use of the work thus protected is subject to copyright or permitted by law under an exception to copyright. Hence, once deployed, TPM may prevent access to, and use of, protected material even in cases where the careful balance of competing proprietary interests on the one hand, and of access and use interests on the other. Moreover, rights holders might even “fence in” material that is either not copyrighted or which is already in the public domain. In Sum, there is a certain danger that TPM will “overrule” the balanced approach which copyright law adopts by balancing proprietary and non-proprietary interests,

quite like too restrictive use conditions in click-through contracts tend to create “private legislation”.¹³⁰⁰

The question then is to what extent TPM should be protected by law against their circumvention. Basically, two options are available. One option is to protect technical protection measures only to the extent to which they protect copyrighted material and uses not covered by exceptions to the exclusive right. Of course, such a protection would be almost meaningless. The other option is to protect technical protection measures under all circumstances. If legal anti-circumvention protection can ever be successful at all, this would be the way to give this protection its utmost effect, at the price, however, of extending it far beyond the balance struck by the copyright legislature. Whereas the WIPO-Treaties only oblige Member States to “provide adequate legal protection and effective legal remedies against the circumvention of effective technology measures [...] that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law”,¹³⁰¹ the EU-Copyright Directive and consequently the Amendment of the German Copyright Act, however, grant a legal protection for TPM which goes beyond the minimum requirement as set by the WIPO-Treaties.

According to § 95a (1) of the German Copyright Act effective TPM may not be circumvented without the prior permission by the rights holder. TPM are defined as technologies, devices or components that, in the normal course of their operation, are designed to prevent or restrict acts, in respect of works or other subject matter protected by the Copyright Act. They are deemed “effective” if the use of a protected work or other subject-matter protected by the Copyright Act is controlled by the rights holders through application of an access control or protection process, such as encryption, scrambling or other transformation or a copy control mechanism, which achieves the protection objective.¹³⁰² Furthermore, certain preparatory acts, such as manufacture, import, distribution, sale, rental, advertisement for sale or rental or possession for commercial purposes of devices, products or components or the provision of services related to the circumvention of effective TPM are prohibited.¹³⁰³ It shall only briefly be noted that, in addition, § 95c of the German Copyright Act implements Art. 7 of the EU-Copyright Directive, according to which the removal or alteration of any electronic rights-management information is prohibited.¹³⁰⁴

The obligation to provide “adequate legal protection” against the circumvention of any effective TPM¹³⁰⁵ was implemented by the German legislator by providing — in addition to civil law injunctive relief — a criminal sanction, according

¹³⁰⁰ See: Lessig (1999): 130, 135. Elkin-Koren (1998): 1295, 1315 et seq. Vinje (1996b): 431, 437. Bechtold (2002): 370.

¹³⁰¹ Art. 11 WCT and Art. 18 WPPT.

¹³⁰² § 95 (2) of the German Copyright Act; Art. 6 (3) of the EU-Copyright Directive.

¹³⁰³ For details see: § 95 (3) of the German Copyright Act; Art. 6 (2) of the EU-Copyright Directive.

¹³⁰⁴ For details see: § 95c of the German Copyright Act.

¹³⁰⁵ Art. 6 (1) of the EU-Copyright Directive.

to which the circumvention or certain preparatory acts may be sanctioned with imprisonment of up to one year or a fine, if the act is done for other than an exclusively private use of the offender or for closely related persons.¹³⁰⁶ The removal or alteration of any electronic rights-management information is subjected to the same provision.

§ 95b of the German Copyright Act contains the exceptions to the legal anticircumvention protection that shall ensure that beneficiaries of certain exceptions may actually benefit from those exceptions. However, in line with Art. 6 (4) (4) of the EU-Copyright Directive, § 95b of the German Copyright Act only applies in the case of off-line distribution and as far as certain important public policy exceptions are concerned that are explicitly listed. In those cases the rights holders are obliged to provide “necessary means” to the beneficiaries in order to make use of the exceptions to the extent necessary. If the rights holders fail to do so, civil actions may be taken by the beneficiaries of the exceptions listed in § 95b of the German Copyright Act. Furthermore, the rights holder may be sanctioned with an administrative fine of up to €100,000.¹³⁰⁷ However, the legislator has left it open what a “necessary means” could be and in which way or form they have to be provided to the beneficiaries of the exceptions.

However, according to § 95b (3) of the German Copyright Act no comparable obligation of rights holders exists in cases where copyrighted material is made available to the public online on contractually agreed terms. In other words, in these cases TPM and the legal protection granted to them override all exceptions and limitations. This is even true in the case of exceptions or limitations which protect particularly high-valued interests and rights, such as the freedom of news reporting, public discussion by way of citation and the like. At the present time, it is difficult to predict the effect of this far-reaching protection for the future information society. According to the Directive, the EU-commission is under a duty to monitor the future development carefully. At any rate, for the time being, this broad protection may encourage rights holder to shift the distribution of their contents to online-distribution.

In addition, in an attempt to protect consumers, § 95d of the German Copyright Act provides that works and other subject matter protected by TPM have to bear a label describing the characteristics of the TPM applied. A violation of this provision is subject to an administrative sanction.¹³⁰⁸ However, it should also be noted that if labeled correctly, it will be rather difficult for the purchaser to assert a claim for the TPM-protected goods being defective,¹³⁰⁹ e.g. in cases where a CD is not playable on the CD-drive of a PC.

Some further comments seem to be called for on this subject.

First, regarding the private use exception of § 53 of the German Copyright Act, only reproductions on to paper or any similar medium and reproductions made

¹³⁰⁶ § 108b of the German Copyright Act.

¹³⁰⁷ § 111a (2) of the German Copyright Act.

¹³⁰⁸ § 111a of the German Copyright Act.

¹³⁰⁹ §§ 434 et. seq. of the German Civil Code.

for scientific or non-commercial archival purposes are embraced by § 95b of the German Copyright Act. This means that only these limited exceptions enjoy priority over the application of TPM. Due to the need of further examination and discussion, the legislator has left it to a future amendment, whether to make use of the optional provision of Art. 6 (4) (2) of the EU-Copyright Directive, according to which Member States may take appropriate measures to ensure that beneficiaries of the private use exception can also make digital copies of works protected by TPM. For the time being, this means that if TPM are applied and if no voluntary measures are taken by the rights holders, private copies cannot be made legally, even if § 53 (1) German Copyright Act entitles to do so.

Second, other than in the U.S.¹³¹⁰, in Germany no entitlement to self-help (“right to hack”) was introduced into the Copyright Act. This raises some interesting questions, for example how to access works protected by TPM that have fallen into the public domain. True, legal protection against anticircumvention of TPM is only granted in respect of works or other subject matter protected by copyright.¹³¹¹ However, the problem is that the devices needed to circumvent non-protected TPM can invariably also be used to circumvent protected subject matter and therefore conflict with the provisions of § 95a (3) of the German Copyright Act.

Third, yet another question is how access to protected works protected by TPM, which is allowed for the beneficiaries listed in § 95b of the German Copyright Act, is to be reconciled with with the legal protection of services based on, or consisting of, conditional access as granted by the Act on Conditional Access¹³¹², that does not include any limitations on the right to control access.¹³¹³ Of course, at present the practical implications of a possible overlap seem to be rather limited, since according to § 95b (3) of the German Copyright Act, in the online environment, where access controlled services are most likely to be found, TPM override all access “rights” which beneficiaries might have under a copyright exception.

Finally, the broad legal protection granted to TPM tends to conflict with the system of lump-sum levies and its application in regard to digital storing and copying devices. If digital storing and copying devices will be deemed subject to lump-sum levy payments, the legislature should make use of Art. 6 (4) (2)

¹³¹⁰ 17 U.S.C. § 1201.

¹³¹¹ § 95a (2) of the German Copyright Act; Art. 6 (3) of the EU-Copyright Directive.

¹³¹² Gesetz über den Schutz von zugangskontrollierten Diensten und von Zugangskontroldiensten (Zugangskontroldiensteschutz-Gesetz — ZKDSG), German O.J., 2002-I, 1090. This Act implemented the EU-Directive 98/84/EC of the European Parliament and the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access into national law. Regarding the implementation see: Bär, Hoffmann (2002): 654.

¹³¹³ However, Recital 21 of the corresponding EU-Directive 98/84/EC states that the Directive is without prejudice to the application of Community rules concerning intellectual property rights.

Copyright Directive and ensure that — at least to a certain extent — private copies can actually be made.

IV The Future

What will the future hold for German copyright law? Of course, the future of copyright is subject to many uncertainties.

However, seen from the present point of view, one of, if not the most prominent question is what will be the appropriate scope of the private use exception in the digital and networked environment. As has already been pointed out, the answer to this question is interrelated with the use and effect of TPM. For the time being, copyright law in Germany gives TPM priority over the possibility to make copies for private uses and therefore leaves it up to the rights holders, by way of applying copy or access control mechanisms, to prevent acts of digital private copying. However, the German legislature might make use of Art. 6 (4) (2) of the EU–Copyright Directive and oblige rights holders to make available to the beneficiaries of the private use exception the means necessary so that they can effectively benefit from the private use exception. Also, if digital equipment and especially blank digital storage media will indeed be found subject to the levy system of §§ 54 et seq. of the German Copyright Act, then the making of copies for private use should not be prevented by TPM. However, due to the higher intensity of use, the lump–sum payments made for digital equipment and storage media would have to be considerably higher than they are with regard to analog copies. But then, the current debate on a levy for PC–hard disks has demonstrated that even a sum which rights holders consider rather low — and which would probably send the “wrong signal” that copying whole works is legal — is claimed to be too burdensome by hardware manufacturers. In addition, at present the role of collecting societies is linked to the continuing existence of lump–sum payments that the collecting societies have a mandate to collect. If these levies should disappear, the collecting societies will have to look for other roles, offer other services and assume other tasks with regard to the exploitation of copyrighted works.

As is revealed by the uncertainty regarding the future of the private use exception, its conditions and justifications will have to be further explored. Of course, this is not an easy task since the private use exception benefits a large number of individuals that may have quite diverse economic interests. To the extent to which the private use exception is based on market failure, it might indeed lose part of its legitimacy due to TPM/DRM–systems. Also, it should not be overlooked that any law which implements a regulation which contradicts the prevailing notions shared by the general public about what is right and what is wrong, is counterproductive and bears the risk to erode the credibility of the legal system as such. The same is true for laws that cannot be sufficiently enforced.

Of course, in a certain way, DRM serves the same purpose as copyright in making information goods exclusive and thus marketable.¹³¹⁴ DRM facilitates the acquisition of rights, reduce transaction costs and allow a better price differentiation by permitting the rights holder to tailor their products and the prices to the individual needs of the users. It is claimed that users get offered a greater choice, that rights holders can better exploit the markets for their products and that, ultimately, DRM secured by TPM will increase the overall public benefit.¹³¹⁵ Of course, in a perfect system of DRM, the combination of contract and technology could lead to a level of protection never granted by traditional copyright,¹³¹⁶ nor even by the possibility to extend copyright by way of contractual provisions in the form of preformulated mass-market standard terms and conditions.¹³¹⁷ This may lead to contradictions between the former scope of legal protection by Copyright and the scope of protection possible through DRM. Thus, DRM-systems may pose a threat to the finely tuned copyright system as we know it and eventually may require a new body of information law to safeguard the public domain.¹³¹⁸

¹³¹⁴ See: Bechtold (2002): 282 et seqs.

¹³¹⁵ For a detailed discussion see: Einhorn (2002): 82. It should be noted, however, that not all economists share the same view; for a critical approach see: Benkler (1999).

¹³¹⁶ See: Peukert (2002): 689, 696.

¹³¹⁷ For discussion of the US–Uniform Computer Information Transactions Act (UCITA) see: Lejeune (2001). And for discussion of the implications under German law see: Dreier, Senftleben (2001).

¹³¹⁸ See: Bechtold (2002): 385. Hugenholtz (2000b).

4.3.2 Copy Protection by DRM in the EU and Germany: Legal Aspects

*Bettina Goldmann*¹³¹⁹

I Introduction

During the last couple of years, private copying of music CDs and files has become more and more popular, and the phonographic industry is experiencing significant losses in sales figures. Today, not only music, but also films, books and other digital media content is being made available on the web. Copying has become a common tool for the enjoyment of copyrighted works now so readily available without going to a store and purchasing the product.

However, the industry has started to fight back against the continuing appropriation of their copyright-protected material by using various technologies. These allow content owners to protect their copyright and to have direct contact with customers. These “digital rights management mechanisms” (hereafter “DRM”) use digital technology in order to administer rights in copyrighted subject matter. DRM function at present in particular by way of Technological Protection Measures (hereafter “TPM”), which means all technical tools which are designed to prevent acts of access to, or use of copyrighted subject matter without authorization. Often, these TPM encrypt digital media content and limit access only to those people who have acquired a proper license, or completely prevent copying or storing of the work. The comments herein on the legal framework of DRM will deal especially with DRM — and, within this framework, particularly TPM — which prevent copying, i.e. which lock-up content.

Currently, a number of copy protection measures such as “Key2Audio” or “Cactus Data Shield 200” have been brought into use to impede the copying of audio CDs via the CD-Rom drive of a Personal Computer and the industry is working to refine and perfect these measures.

Regarding films on videocassettes, the Macrovision copy protection has been in place already for 10 years and impedes the private copying of analogue videocassettes.¹³²⁰ DVD are also protected by the industry through various TPM which impede analogue private copies. Digital copying is prevented by the “Content Scramble System (CSS)”, which encodes the digital content of a DVD and inhibits digital copying. DVD-players or computer software for watching DVDs have the CSS source code integrated and are thus able to make the content visible, but without offering an opportunity to copy.¹³²¹ DRM can also be designed

¹³¹⁹ Attorney-at-law Baker & McKenzie London and Munich.

¹³²⁰ See: <http://www.macrovision.com/solutions/video/copyprotect/>, last visited March 14, 2003 for a comprehensive overview over the functionalities.

¹³²¹ See in more detail: Knies (2003).

which prevent copying of content made available in a non-tangible form, (i.e. via the World Wide Web), to prevent or regulate download and printing.

The German Copyright Act (“*Urheberrechtsgesetz*”— hereafter “*GCA*”), like most other European copyright legislation, grants the individual user an exception to allow — within certain boundaries — copying for non-commercial, private purposes. However, there is an obvious conflict between the industry’s intention to protect its content, and the individual consumer’s interest in making private copies as permitted by law. Since today’s digital technology enables the copier to produce a clone (i.e. an identical copy of a copyrighted work without any loss of quality), copying is far more dangerous than during the age of analogue technology when copies were only imperfect versions and not able to substitute for the original (e.g., the recording of an audio CD on an analogue audio tape).

There are opposing interests between those who bear the financial risk of producing movies, audio recordings and other content, and those who wish to copy — often legitimately. The dilemma of reconciling cultural interests, especially the free flow of information, on the one hand and, on the other, remuneration of rightsholders and protection of content, has now been addressed by the EU “*Directive 2001/29/EC on The Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society*” (hereafter “*Directive*”), which should have been re-enacted in the national law of all Member States by the end of 2002. In Germany, the “*Act Relating to Copyright in the Information Society*”¹³²² (hereafter the “*Act*”) re-enacts the Directive.¹³²³ The German Copyright Act as it shall be amended by the *Act Relating to Copyright in the Information Society* shall hereafter be referred to as “*New German Copyright Act*” (“*NGCA*”), in contrast to the German Copyright Act before implementation of the Directive (hereafter “*Previous German Copyright Act*” — “*PGCA*”).

So far only Greece, Italy and Denmark have implemented the Directive.¹³²⁴ All other Member States are late and were not able to meet the implementation deadline.

This article will focus exclusively on the regime for private copying and its relationship to DRM without discussing other aspects of the new legislation and will proceed as follows:

¹³²² The legislative bill and all related documents to the *Act Relating to Copyright in the Information Society*, i.e. the statements of the different interested parties can be accessed at <http://www.urheberrecht.org/topic/Info-RiLi/>, last visited June 3, 2003.

¹³²³ Upon finalization of the manuscript of this article beginning of June 2003, only the version voted by the German Parliament (*Bundestag*) was published and accessible at: http://www.urheberrecht.org/topic/Info-RiLi/ent/Bundesrat_Drucksache.271.03.pdf, last visited June 3, 2003. Whether slight subsequent changes affecting the topic of this article were introduced into the Act before vote in the Federal Council (*Bundesrat*), and when the Act came or shall come into effect was not known upon finalization of this article and could not be taken into account.

¹³²⁴ For the actual status of implementation see: <http://wiki.ael.be/index.php/EUCD-Status>, last visited June 3, 2003.

- II Analysis of the legal situation relating to private copying under the Previous German Copyright Act,
- III The legal framework provided for EU Member States by the Directive,
- IV The implementation of the Directive into the German Copyright Act,
- V Final remarks.

II Legal Situation under the Previous German Copyright Act before Implementation of the Directive

II.1 Private Copying Exception

The GCA has since its enactment in 1965 known an exception for private copying and more and more refined the legal framework for private copies throughout the years. Most of the rules for private copying will continue to apply as well under the NGCA which re-enacts the requirements of the Directive. Private copying — as to be discussed below in more detail — only undergoes slight modifications.

Section 16 GCA grants the author exclusive rights to reproduce the copyrighted work. Section 53, Para. 1 GCA (hereafter “Private Copying Exception”) limits this right by allowing some very specific copying of copyrighted works without the consent of the author, inter alia, under the private copying exception which permits “*single copies of the work for private use*”. This principle remains unchanged under the NGCA. Although Section 53, Para. 1 PGCA, present wording of which dated back to 1985, did not expressly mention the technology used to make copies, the prevailing legal opinion held that the broad language of the Private Copying Exception covered digital copies as well.¹³²⁵ The motivation for introducing the Private Copying Exception in 1985 was linked to the upcoming taping of music and the introduction of reprography technology. It was realised that such actions, which occurred mostly within the private sphere of the individual consumer, could not be effectively controlled and sanctioned. Maintaining the exclusive right of the author in this respect would have led to criminalizing large parts of the population and the need to intrude into the privacy of users to monitor illegal private copying. This rationale is even more true today with internet users mostly downloading content in the privacy of their homes.

In exchange for the use of their works under the Private Copying Exception, authors were under the PGCA — and continue to be under the NGCA — entitled to an “equitable remuneration” pursuant to Sections 54 and 54a GCA¹³²⁶. This equitable remuneration is implemented by means of a blanket compensation for private use of copyright-protected works pursuant to more detailed

¹³²⁵ Decision of the Regional Court (LG) Stuttgart dated June 21, 2001, Computer und Recht 2001, 581 — *Remuneration duty for CD burners*; Schricker, Dreier, Katzenberger, v. Lewinski (1997): 165; Schricker (1999): § 54, note 9; Fromm, Nordemann (1998): §§ 54, 54a, note 2; Möhring, Nicolini (2000): § 54, note 26; Wandtke, Bullinger (2002): § 54, note 4, 5; Schack (2002): 497, 498; Goldmann, Liepe: 37, 39; Knies (2002): 793, 794; Flechsig (2001): 656, 659; Winghardt (2002): 349, 353.

regulations in Sections 54 — 54h GCA and paid in the form of a copyright levy. The levies are paid by the manufacturers, importers and dealers of taping equipment or blank-storage-media. Thus, there is a shift away from the duty of the true consumer to remunerate the author of the copyrighted work to those who commercialise the sale of the relevant taping equipment. In practice, the manufacturers or importers regularly pass on the levy paid to the consumer by raising the price of the equipment or blank-storage-media accordingly, if the pricing of the equipment is not already too low to do so. The Copyright Collecting Societies are exclusively entitled to collect the copyright levies from the hardware and blank-storage-media industry on behalf of authors and publishers, who have assigned their respective remuneration rights to them, and then distribute the revenue under an allocation formula to the rightsholders.¹³²⁷ Copyright levies for audio and video reproduction equipment and blank media are collected by the ZPÜ (“*Zentralstelle für private Überspielungsrechte*”), an organization set up by a number of Copyright Collecting Societies for this task. Copyright levies for reprographic equipment are collected by the Copyright Collecting Society VG Wort.

The wording of Sections 54 and 54a PGCA provided only for copyright levies on audio and video recording equipment or reprographic copying equipment. During the past few years, copyright levies under these provisions have been extended by individual test cases to CD burners, readerprinters, scanners, fax machines, and other modern electronic equipment¹³²⁸, as well as the corresponding electronic storage media (e.g., CDs, CD-ROMs, discs). Decisions on the applicability and adequacy of a tariff are made in the first instance by a specialized Arbitration Panel¹³²⁹ located at the German Patent and Trademark Office. The German Patent and Trademark Office is the supervising authority for the Copyright Collecting Societies. Thereafter, cases can be referred to the civil courts.¹³³⁰ Several lawsuits between the industry and the Copyright Collecting Societies on levies to be paid for PCs and printers are still pending.¹³³¹

¹³²⁶ Section 54, Para. 1 introduces a remuneration claim for all reproductions; Section 54a, Para. 1 and 2 a remuneration claim specifically for reprographic copying.

¹³²⁷ See: Section 54h GCA.

¹³²⁸ See decision of German Supreme Court (*BGH*) NJW 1993, 2118 — *Reader-printer*; decision of the Regional Court (*LG*) Stuttgart dated June 21, 2001, Computer und Recht 2001, 581 — *Remuneration duty for CD burners*; Higher Regional Court (*OLG*) Cologne, Computer und Recht 1997, 482 and Higher Regional Court (*OLG*) Zweibrücken, Computer und Recht 1997, 348 regarding fax machines; Regional Court (*LG*) Düsseldorf ZUM-RD 1997, 513 regarding scanners).

¹³²⁹ “*Schiedsstelle für Urheberrechtsstreitfälle*” pursuant to Section 14 et seq. Copyright Administration Act (*Urheberrechtswahrnehmungsgesetz*).

¹³³⁰ Addressing the Arbitration Panel located in the German Patent and Trademark Office is a preliminary requisite for proceeding with the courts in matters which regard the applicability and the adequacy of tariffs imposed by the Copyright Collecting Societies, compare Section 16, Para. 1 Copyright Administration Act.

The tariffs of the copyright levies, which are only for classic reproduction equipment set out in an Annex to Section 54d PGCA, have not changed since 1985 despite frequent criticism that they have ceased to provide equitable remuneration for authors. Three years ago, as a reaction to criticism, the German government initiated an expert's report on the need to adapt copyright levies to the requirements of the digital age. This "Report of the German Government on the Development of Copyright Levies Pursuant to Section 54 et seq. GCA" ("*2. Vergütungsbericht*") dated July 11, 2000¹³³², confirms that the tariffs for copyright levies are out-of-date and that there is need to take action and to moderately raise levies. Given the outdated distinction between audio and video taping equipment in Section 54 and the Annex to Section 54d GCA, the Copyright Collecting Societies have, during the last years, been able to fix by themselves, and in a more or less arbitrary manner, the tariffs for modern taping equipment, such as fax machines or CD burners, which do not clearly fall into the legal categories of taping equipment. Economic parameters, e.g., statistical studies as to what extent equipment is really used for copying protected content or assessing the losses suffered by the content industry, hardly play a role when fixing these tariffs for copyright levies.

Regarding the scope of private copying, both the courts and legal commentators have had sufficient opportunity during the past decades to interpret and further define the scope of the Private Copying Exception under the PGCA. Briefly, under German law, use qualifies as "private" if only personal needs are satisfied, e.g., if a copy of a CD is made by the buyer for back-up purposes or for listening in their car, or for close friends or family. It remained unclear how many copies would still qualify as "individual copies" under the law. However, for classic paper photocopies, the German Supreme Court had ruled that 7 copies is the limit¹³³³, this number is generally considered too generous for digital copies.

Already under the PGCA, commercial use of the copyrighted work was excluded from the scope of the Private Copying Exception, i.e. sale, swapping copies or giving copies away to foreigners who do not qualify as friends or family (e.g., in peer-to-peer filesharing systems). Under the present law, the copier need not have acquired the "mastercopy" of the copyrighted work from which the copy is made, although the copy must not be, e.g., stolen. Thus, anyone could lawfully borrow a CD from a friend to make a copy for themselves. Given the lack

¹³³¹ See, e.g., press information from BITKOM (German Association of Information Business, Telecommunications and New Media), February 4, 2003 re decision at first instance on Copyright Levies for PCs. The information can be accessed via the "press" section at <http://www.bitkom.org/>, last visited March 18, 2003.

¹³³² "*Second Report of the German Government Regarding the Development of Copyright Levies pursuant to Sections 54 et seq. GCA*", published in *Bundestagsdrucksache* 14/3972, hereafter "2nd Copyright Levy Report".

¹³³³ Decision of the German Supreme Court (*BGH*), GRUR 1978, 474, 476 — *Vervielfältigungsstücke*.

of restrictions in the wording of Section 53, Para. 1 PGCA, private copies made from stolen or illegal copies also came under the Private Copying Exception.¹³³⁴

II.2 No Legal Claim to Private Copying

German copyright law does, according to the prevailing opinion, not give a legal right to private copying, i.e. the user only benefit from a privilege which allows them to make private copies within the boundaries of the legal Private Copying Exception. They have no legal right to do so, although some commentators hold the view that there is such a legal right¹³³⁵ and also representatives of the German Ministry of Justice have recently talked of the “legal right to private copying”.¹³³⁶ If one is to follow the prevailing opinion, the industry is — as a general rule — fully entitled to obstruct the user in making private copies by TPM — even if the user only intends copying within the permitted boundaries. The rightsholder has entire discretion how they choose to make their work available. No legal claim to copying can be construed from the mere privilege the user is given under Section 53, Para. 1 PGCA.¹³³⁷ This rule will remain to be valid under the NGCA.

III Copy Protection and DRM under the EU Directive — “Copyright in the Information Society”

III.1 The Rules for Private Copying under the Directive

The Directive leaves it open for Member States to choose whether or not they want a Private Copying Exception at all. Article 5, Para. 2, differentiates between reprography¹³³⁸ and other private copies but does not, under “other private copies”, differentiate between digital and analogue. Article 5, Para. 2 lit. (b) of the Directive stipulates that if Member States introduce a Private Copy-

¹³³⁴ However, according to prevailing legal doctrine, the additional unwritten criteria must be applied that private copies from stolen copies are illegal, see decision of Higher Regional Court of Berlin (KG), GRUR 1992, 168 — *Dia-Kopien*; Fromm, Nordemann (1998): § 53, note 4; Möhring, Nicolini (2000): § 53, note 9; Wandtke, Bullinger (2002): § 53 note 9; Schricker (1999): § 53, note 13.

¹³³⁵ Hoeren, “Copyright and Consumer Protection – Thoughts regarding the Act on Copyright in the Information Society”, Expert Opinion for the VZBV (*Verbraucherzentrale Bundesverband e.V.* [Organisation for Protection of Consumer’s Rights]), page 23. The Expert Opinion of Hoeren can be downloaded from http://www.vzbv.de/home/start/index.php?page=presse&bereichs_id=&themen_id=&mit_id=180&task=mithttp://www.vzbv.de/start/index.phtml?page=themen&bereichs_id=1&themen_id=3&dok_id=154, last visited May 26, 2003; Knies (2002): 793.

¹³³⁶ See hereto in more detail: Goldmann, Liepe (2002): 362, 364 et seq., footnotes 29 and 30.

¹³³⁷ In more detail: v. Diemar (2002): 587 et seq.; also: Goldmann, Liepe (2002): 362, 365; holding a different view Hoeren, see above footnote 1335.

¹³³⁸ Article 5, Para. 2 lit. (a) of the Directive specifically exempts photocopying of sheet music from the scope of admissible private copying exceptions.

ing Exception, they have to ensure “fair compensation” for the rightsholder. How this “fair compensation” requirement should be interpreted is explained in Recital (35) of the Directive, which states that the Member States should take into consideration (i) the possible harm to the rightsholder, (ii) the degree to which TPM are used and (iii) whether the rightsholder has already received payment in some other form. Recitals, however, generally serve only as an interpretation guideline for the text of the Directive, and only as a recommendation to Member States on what aspects may be taken into account. They are therefore non-binding. They summarise the discussion points which arose while the Directive was being drafted, but also show that these aspects were not agreed between the Member States, otherwise the wording would have been reflected in the body of the Directive itself.

The duty to grant rightsholders “fair compensation” is not identical with the German notion of “equitable remuneration” and does not oblige those countries who do not have a copyright levy to introduce such a system.¹³³⁹ The notion of “fair compensation” is, in fact, the result of a compromise between countries already providing a system of “equitable remuneration” for rightsholders and those which have, in the past, been strictly against it, namely Great Britain and Ireland.¹³⁴⁰ These countries are not bound by the Directive to introduce copyright levies, but may ensure “fair compensation” by other means.

The Directive, in general, encourages the development of individual licensing systems and the use of TPM, e.g., in Recital (55) et seq. and Article 7 of the Directive. Moreover, the Directive makes it clear that the availability of DRM requires the copyright levy systems to be gradually phased out. This is because copyright management systems make it possible to compensate rightsholders accurately and directly for the particular use to which the work has been put. Were levies to coexist with such measures, rightsholders could control private copying and claim direct remuneration from users as well as being compensated by copyright levies.¹³⁴¹

III.2 Protection of DRM

Apart from the private copying issue, the Directive addresses DRM explicitly in its provisions for the protection of TPM themselves.

In brief, pursuant to Article 6 of the Directive, the Member States will (1) provide adequate legal protection against the intentional circumvention of effective technological measures and (2) provide adequate legal protection against certain preparatory actions, e.g., manufacturing, import, distribution, sale, rental, advertisement or possession for commercial purposes of devices which are aimed at the circumvention of effective TPM. Article 6, Para. 3 contains the defini-

¹³³⁹ Recital (35) of the Directive provides interpretation guidelines how the European Commission wishes the notion of “fair compensation” to be understood.

¹³⁴⁰ See: Reinbothe (2001a): 733, 738.

¹³⁴¹ See: Recital (35) of the Directive stating that double payment should be avoided; Huppertz (2002): 105, 108.

tion of “effectiveness”, clarifying that “effectiveness” under the Directive does not, contrary to the general understanding, mean that TPM must be 100% effective — otherwise it would not be necessary to protect them legally against circumvention. It suffices that the measure is “*in the normal course of its operation*” designed to prevent or restrict acts which are not authorised by the rightsholder. Thus it is not required that these devices withstand attempts at hacking or circumvention. As examples of effective TPM, Article 6, Para. 3 mentions “*encryption, scrambling ...*” and other “*copy control mechanisms which achieve the protection objective*”.¹³⁴²

Whereas the use of TPM is encouraged by the Directive, Recital (48) clarifies that rightsholders are not obliged by the Directive to use them to lock up their content.

In Article 7 the Directive provides that Member States must adequately protect information relating to rights management. This means that they must provide reasonable legal protection against persons who intentionally or grossly negligently remove or alter electronic rights-management information or distribute, broadcast, communicate or make available works from which electronic rights-management information has been removed, provided that these activities, *inter alia*, facilitate, enable or conceal copyright infringement.

Finally, by Article 8 of the Directive the Member States are obliged to provide appropriate sanctions and remedies for infringement of rights and obligations set out in the Directive. These include provisions for rightsholders which guarantee access to injunctive relief or possible seizure of infringing material and circumvention tools. Altogether, the Directive introduces a comprehensive system of protection for TPM.

III.3 Relationship between Private Copying and Circumvention of TPM

TPM are suitable for minimizing the dangers to copyright as a result of piracy. However, these measures may also prevent private copying and other uses of copyrighted work which are permitted under statutory law. Thus, notwithstanding the general principle of protection for TPM, obligations have been imposed on the Member States by Article 6, Para. 4 of the Directive: the beneficiaries of limitations and exceptions under Article 5, Para. 2 and 3 of the Directive must in fact be able to use the copyrighted work for the described purpose, although it may be locked-up by TPM and is thus, in principle, inaccessible.¹³⁴³ The Directive suggests that rightsholders adopt voluntary measures and enter into agreements with their respective users, ensuring access to copyrighted works within the boundaries of the legal exceptions. How the relationship between TPM and the limitations and exceptions to copyright are to be solved by the content industry and national legislatures from a practical standpoint, remains

¹³⁴² See in more detail on the anti-circumvention provisions of the Directive: Hupertz (2002): 105, 106 et seq.

¹³⁴³ See Article 6 of the Directive. See also: Kröger (2001): 316, 321 et seq.

open. On the one hand, Member States are obliged to ensure that TPM will not be used vis-à-vis the beneficiaries of certain exceptions.¹³⁴⁴ On the other hand, Member States are entitled, but not obliged, to take measures which ensure that users can benefit from the Private Copying Exception notwithstanding use of any TPM. Here the Directive favours voluntary agreements between rights-holders and users. Only if the agreements fail and private copying has not been made sufficiently possible on a voluntary basis, may the Member States adopt measures to facilitate private copying.¹³⁴⁵ Thus, in the absence of any voluntary solution, the Directive does not require provision of technical means for circumvention to the beneficiaries of the statutory exceptions.¹³⁴⁶ It only offers a possibility for Member States to intervene if rightsholders do not comply with the Private Copying Exception. Article 6, Para. 4 does not apply at all if works are made available on agreed contractual terms in interactive use, e.g., through on-demand services.¹³⁴⁷

Thus, the Directive gives Member States a fairly large amount of discretion over the relationship between private copying and DRM. But the fact that the Member States could not reach agreement on concrete and binding language in the Directive on a European level, also shifts a number of unresolved problems to national legislatures.

IV Implementation of the EU Directive in the German Copyright Act — Is There Sufficient Implementation of the Directive’s Aims?

IV.1 The Legislative Process

The German government introduced the first “Government Draft” (*Regierungsentwurf*) of the “Bill on Regulation of Copyright in the Information Society” on August 16, 2002.¹³⁴⁸ During the legislative process, the Federal Council (*Bundesrat*) made a number of substantial criticisms, notably involving the fact that the copyright levy system had not been substantially changed.¹³⁴⁹ In a

¹³⁴⁴ See Article 6, Para. 4, Subparagraph 1 of the Directive.

¹³⁴⁵ On the criteria to be applied, Recital (52) gives further guidelines. In particular, the “three-step-test” codified in Article 5, Para. 5 of the Directive must be observed. This requires that limitations introduced can only apply to certain special cases; must not conflict with the normal exploitation of the work; and must not unreasonably prejudice the legitimate interests of the rightsholder.

¹³⁴⁶ See: Huppertz (2002): 105, 108.

¹³⁴⁷ Article 6, Para. 4, Subparagraph 4 of the Directive.

¹³⁴⁸ This draft differs substantially from and overrides the older “*First Discussion Draft for the 5th Amendment Act of the German Copyright Act*”, dated July 7, 1998, published in “Kunstrecht und Urheberrecht” 1999, 157 et seq.

¹³⁴⁹ Comments of the Federal Council (*Stellungnahme des Bundesrates*) dated September 27, 2002, published as BT-Drucksache 15/38; the document can be accessed at <http://www.urheberrecht.org/topic/Info-RiLi/>, last visited March 18, 2003.

Replica¹³⁵⁰ dated November 6, 2002 the federal government rejected most of these arguments, especially those on the provisions to be adopted for private copying and TPM, defended its original approach and, on the same day, published the Copyright Bill¹³⁵¹ which only slightly deviated from the previous Government Draft.

The Copyright Bill was then subjected to a lively discussion within the interested circles, namely publishers and rightholders' associations and associations of the equipment industry.¹³⁵² The Copyright Bill has been transferred to the German Parliament (*Deutscher Bundestag*) for voting and was discussed in the Legal Committee (*Rechtsausschuss*) and other committees of the German Parliament. The Legal Committee reported and recommended some changes to the Copyright Bill on April 9, 2003.¹³⁵³ The German Parliament voted on the Copyright Bill in the form as amended in the Legal Committee on April 11, 2003. Then, the Copyright Bill was transferred to the Federal Council on May 2, 2003.¹³⁵⁴ The Federal Council has on May 23, 2003 addressed the Conciliation Committee (*Vermittlungsausschuss*)¹³⁵⁵, in particular since it continues to object to the fact that the Copyright Bill does not restrict private copying to copying from legal sources and that digital private copies can legally be prepared by third parties.

According to the Explanatory Memorandum attached to the Copyright Bill, the urgency of implementation has resulted in a minimum coverage of the Directive's requirements.¹³⁵⁶ Issues which require more extensive study and debate will be left for later legislation. Amongst the topics not addressed in the Copyright Bill are the implementation of Article 6, Para. 4, Subparagraph 2 of the Directive (Enforcement of the Private Copying Exception vis-à-vis the use of TPM). The German government announced its intention to use the opportunity for enactment of further legislation in these areas as well as implementation of the recommendations in the 2nd Copyright Levy Report. This is planned to take place during the current Parliamentary Session. Thus it is to be expected that the legislature will, in the near future, approach the issues and set up new tariffs for copyright levies by way of decree. Alternatively, they may just codify the

¹³⁵⁰ Replica of the German government (*Gegenäußerung der Bundesregierung*) dated November 6, 2002; the document can be accessed at <http://www.urheberrecht.org/topic/Info-RiLi/>, last visited March 18, 2003.

¹³⁵¹ The "Legislative Bill on Regulation of Copyright in the Information Society", published as *Bundestagsdrucksache 15/38*.

¹³⁵² See the various statements at: <http://www.urheberrecht.org/topic/Info-RiLi/>, last visited June 2, 2003. See *Günnewig* within this book on page 528.

¹³⁵³ The text can be accessed at: <http://www.urheberrecht.org/topic/Info-RiLi/ent/1500837.pdf>, last visited June 2, 2003.

¹³⁵⁴ See: http://www.urheberrecht.org/topic/Info-RiLi/ent/Bundesrat_Drucksache_271-03.pdf, last visited June 2, 2003.

¹³⁵⁵ See: <http://www.urheberrecht.org/topic/Info-RiLi/ent/BR-Drs-271-1-03.pdf>, last visited June 2, 2003.

¹³⁵⁶ The time limit for implementation of the Directive in Member States lapsed on December 22, 2002.

principles of “equitable remuneration”, leaving the assessment of the precise tariff to negotiations with ZPÜ and VG Wort.

IV.2 Main Features of the New German Copyright Act as Amended by the Act with Reference to DRM

In the NGCA as in the Directive, DRM are, on the one hand protected by law and on the other, a criteria to be taken into account when considering remuneration of the rightsholders under the copyright levy scheme. However, the Act does not make use of the term DRM in general, but refers — like the Directive — only to TPM.

The Act re-enacts Article 6 of the Directive very closely by introducing new Sections 95a and 95b. Briefly, Section 95a NGCA will prohibit circumvention, or acts preparatory to circumvention, of effective TPM. The definition of “effective technological measures” follows exactly the wording of Article 6, Para. 3 of the Directive. Section 95c NGCA implements Article 7 of the Directive and, again, follows the wording of the Directive closely by prohibiting the removal of rights management information. Sections 108b and 111a NGCA provide for criminal and administrative sanctions in case of infringement in order to ensure the effective protection of TPM. In addition to the provisions introduced on the basis of the Directive, a new Section 95d NGCA will oblige the rightsholder to identify, for reasons of consumer protection, the use of TPM and their effects on the use of the copy of the work.¹³⁵⁷

Section 95b NGCA implements Article 6, Para. 4 of the Directive in a “complex and somewhat burdensome provision”¹³⁵⁸, but proposes only measures where the intervention by Member States is mandatory. Thus, the mandatory enforcement of reprographic copying as provided by Article 6, Para. 4 Subparagraph 1 is reflected in Section 95b, Para. 1 NGCA. The difficult issue of the relationship between private copying in general and use of TPM in Article 6, Para. 4, Subparagraph 2 is, however, not addressed. It is planned that this topic will be after detailed examination and discussion subject of later legislation.

IV.3 Private Copying under the NGCA

Under the NGCA as amended by the Act, the Private Copying Exception in Section 53, Para. 1 remains as broad as it was under the PGCA. In particular, the Private Copying Exception now explicitly covers analogue as well as digital copies without making any distinction between them. This in spite of the fact that Recital (38) of the Directive explicitly suggests “[...] *due account should be taken of the differences between digital and analogue private copying and a*

¹³⁵⁷ This provision is not based on the Directive, but rather on the practical experiences made with copy protection systems, especially audio CDs, which do not allow the CD to be played on certain CD-players or disc-drives of PCs and has led to substantial criticism from the customer side. See hereto: Goldmann, Liepe (2002): 362 et seq.

¹³⁵⁸ See: Huppertz (2002): 105, 110.

distinction should be made in certain respects between them". Given the more interpretative and explanatory character of the Recitals, it cannot be said that German law is in violation of the Directive on this point, since Article 5, Para. 2, lit. (b) of the Directive allows copies "on any medium" without mandatory distinction between analogue and digital copies.¹³⁵⁹

In all other respects, the Private Copying Exception has not been substantially changed either. In particular, its scope has not been narrowed by requiring that the original must be owned by the copier. The new wording clarifies that private copies may serve neither directly nor indirectly for pecuniary reward. The requirement that no remuneration must be paid for copies which are prepared by another person which before only applied to copies of audiovisual content and sound recordings, now applies in general, thus also for digital copies. Only reprographic copies which are made by photomechanical process can be prepared by third parties against payment. Since the new Section 53, Para. 1 does not contain any further restrictions, copies can also be made from second, third or even later generations of a reproduction and there will be no requirement that copying is only possible from lawful sources, (i.e. no prohibition of copying from pirated material), as requested by the rightsholders¹³⁶⁰ and suggested by the Federal Council.¹³⁶¹

IV.4 The Principle of "Equitable Remuneration" vs. "Fair Compensation" under the Directive

The Act does not introduce any changes to the existing principle under German copyright law set forth in Sections 54 et seq. that rightsholders have a right to "equitable remuneration" for private copies of their copyrighted works and that this "equitable remuneration" is effected by the copyright levies collected by the ZPÜ. In fact, the language of Sections 54, 54a GCA and of the Annex to Section 54d GCA, in which tariffs for copyright levies are fixed, remains entirely as it was under the PGCA.

The question arises whether this existing "equitable remuneration" principle still conforms with the "fair compensation" requirement as it is stipulated and interpreted by the Directive. The commissioner *Frits Bolkestein* explained, in

¹³⁵⁹ However, the Federal Council has specifically objected to that fact that no distinction is made between analogue and digital copies in the Copyright Bill.

¹³⁶⁰ Under the name "Forum of Rightsholders", important representatives of rightsholders, inter alia *Bertelsmann AG*, *Börsenverein des Deutschen Buchhandels e. V.* (Association of the German Book Traders), *Bundesverband der Phonographischen Wirtschaft e. V.* (German Association of the Phonographic Industry), IFPI (*International Federation of the Phonographic Industry*), *Deutscher Musikverleger-Verband* (*German Music Publisher's Association*) and the various German Copyright Collecting Societies have advocated a joint position on the Bill; the statement of the Forum of Rightsholders dated October 2002 can be accessed via <http://www.ifpi.de> under the legal section of the website, last visited June 3, 2003.

¹³⁶¹ Upon completion of this article, it had not been decided whether the Federal Council could still achieve a legislative change in this point.

answer to a parliamentary question raised in the European Parliament on March 26, 2002, that “fair compensation” would be a “new concept”.¹³⁶² However, this statement should be interpreted as meaning a “new concept” at the level of European harmonisation since for the first time all Member States, including those which have so far rejected a copyright levy system, are obliged to grant the author some sort of fair remuneration for private copying. Further, *Jörg Reinbothe*, one of the authors of the Directive, has confirmed that, given the principle of “equitable remuneration” under German law, there would be no need to adapt because the law already gave the rightsholder more than fair compensation.¹³⁶³

On the other hand, as mentioned above, Recital (35) gives specific guidelines on how the term “fair compensation” should be interpreted. Thus, when determining the level of fair compensation, valuable criteria to be taken into account “would be” (i) possible harm to the rightsholder and (ii) whether the rightsholder has already received payment for copying in some other form. Moreover, in certain cases, where there is only minimal prejudice to the rightsholder, there would be no obligation to pay.¹³⁶⁴ So far, the German levy system has not taken into account these criteria, and copyright levies for modern taping equipment are fixed more or less arbitrarily by the Copyright Collecting Societies, without obligation to render accounts for the tariffs used.

However, given the fact that these criteria are not in the body of the Directive, but only in Recital (35) and are therefore not binding on how “fair compensation” must be assessed in the Member States, it will be difficult to argue that the German levy system violates the “fair compensation” requirement as set out by the Directive.

IV.5 Taking into Account TPM

Article 5, Para. 2, lit. (b) of the Directive rules that fair compensation must take account of the application or non-application of the TPM referred to in Article 6 of the Directive. This obligation of the Member States is confirmed in Recital (35), “[...] *the level of fair compensation should take full account of the degree of use of technological protection measures*”.

The Act implements this requirement by introducing a new Section 13, Para. 4 into the Copyright Administration Act (*Urheberrechtswahrnehmungsgesetz*),

¹³⁶² The document can be accessed via http://europa.eu.int/eur-lex/en/search/search_epq.html under the section “Parliamentary Questions”, last visited June 3, 2003.

¹³⁶³ See: Reinbothe (2002): 43, 49.

¹³⁶⁴ The European Commission has confirmed, for example, that mere “time-shift” copies, which cannot be kept, but are exclusively designed to be watched once at a later point of time, no duty of payment will arise, since the normal exploitation of the work will not be endangered (Declaration to the Protocol of the European Council on Recital (35)). England plans to introduce this exception for time-shifting replay according to its draft legislation, which can be accessed under <http://www.patent.gov.uk/about/consultations/eccopyright/>, last visited March 17, 2003.

which governs the rights and obligations of all Copyright Collecting Societies. This paragraph reads: “*When creating tariffs which are based on Sections 54 and 54a of the GCA, it must be taken into account to what extent technological protection measures pursuant to Section 95a of the GCA are applied to the respective works or the respective protected subject-matter.*” According to the Copyright Bill’s Explanatory Memorandum, this allows a more flexible reaction to the development of TPM than fixing tariffs by legislation.

Here, the question arises whether Germany has sufficiently re-enacted the Directive by providing for a mere instruction to the Copyright Collecting Societies to take into account the use of TPM, without further guidelines as to how and when this should be done. Thus, it will for now be entirely within the Copyright Collecting Societies’ power to adjust the tariffs of the copyright levies. Since the copyright levies payable pursuant to Section 54 GCA constitute an important part of the revenue of the Copyright Collecting Societies, it is unlikely that they will voluntarily reduce their tariffs on digital equipment in the near future even if the use of TPM becomes more frequent and the amount of use of such equipment for copying of copyrighted content will diminish.

Since the tariffs of Copyright Collecting Societies are subject to judicial control through the specialized Arbitration Panel, there will be judicial control over the applicability and level of tariffs imposed, provided the taping equipment industry which produces equipment containing or respecting copy protection measures files lawsuits against the tariffs imposed. However, in order to encourage the content and equipment industry to joint efforts for the use of DRM it would have been desirable for the legislation to place the duty to take into account the use of TPM in a more prominent position than in the Copyright Administration Act. The German legislator should also have tackled the issue of reforming the copyright levy system immediately, giving individual licensing systems more incentives to develop. The question also arises whether the German government has looked closely enough at the interpretation guidelines for “fair compensation” in Recital (35). At present the Copyright Collecting Societies are not legally bound to design their tariffs to take into account both the harm to the rightsholder and other possible compensations received. Here, although not in clear violation of the Directive, the Act fails to sufficiently reflect the objectives of the Directive.

Given the upcoming use of DRM, one argument always raised by the Copyright Collecting Societies against reduction of tariffs or exemption of certain equipment, is that no effective, safe TPM presently exist. They claim that all the TPM on the market could easily be circumvented. It remains to be seen how fast the market of reliable TPM will develop. The industry is definitely in a position to act. However, it must be kept in mind that the “effectiveness” of TPM does not mean they must be 100% safe. The wording of Article 6, Para. 3 of the Directive provides that technological measures are devices which in the “normal course of operation”, i.e. not if circumvented or hacked, “[...] *are designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorised by the rightsholder [...]*”. If TPM were only effective when 100% resistant to hacking, there would be no need to protect them by special lan-

guage in the Directive. Moreover, it must be kept in mind that copyright levies are clearly not designed to compensate copyright infringement, i.e. copies made in violation of the Private Copying Exception.¹³⁶⁵ Thus, illegal copies must be attacked by injunctive relief and claims for damages against the violator. Owners of copyrighted software (where private copying continues to remain entirely illegal) must go after violators themselves, although violation of software rights is often difficult to track. Therefore, in practice, rightsholders may often fail to receive compensation for illegal software copying. Thus, the argument raised by the Copyright Collecting Societies is of limited relevance.

Hence, the approach taken in the Act seems disappointing. It shifts to the Copyright Collecting Societies the responsibility for taking into account the application of TPM in their tariffs. It might take some time for the Copyright Collecting Societies to follow this call and accept the new realities. Given the interpretation criteria of “fair compensation” in Recital (35) and the duty of Member States to take the application of TPM into account, it is debatable if the Directive has been adequately re-enacted. However, when looking at the solutions for effective re-enactment of Article 5, Para. 2, lit. (b) of the Directive suggested by other Member States (namely France and the UK), it must be admitted that they definitely lag behind Germany.¹³⁶⁶

V Concluding Remarks and Perspectives

The Directive and the Act provide protection of TPM itself, which deserves approval from a legal standpoint, but the relationship between TPM and private copying in the digital age is a more delicate issue. Striking a balance between the interests of the individual user to make private copies and the legitimate interests of the rightsholders to receive fair compensation for copying remains difficult under the Directive and the New German Copyright Act:

¹³⁶⁵ Explicitly confirmed by the Regional Court of Stuttgart of June 19, 2001 for the application of Copyright Levies on CD burners, published in *Computer und Recht* 2001, 581. Sharing this opinion: Haedicke (2001): 349, 363; Huppertz (2001): 105, 108.

¹³⁶⁶ Looking to the first preparatory documents of a bill for implementation of the Directive in France: the private copying exception will be left unchanged; nothing has been suggested regarding the duty to take into account the application of TPM when fixing remuneration for private copies (see drafting document at <http://www.culture.fr/culture/cspla/avantproj.pdf>, last visited on June 3, 2003). In France, a special “Commission for Private Copies” fixes the rules for the application and level of compensation for private copies (Art. L 311-5 French Intellectual Property Code — *Code de la Propriété Intellectuelle*). In the UK, private copying is allowed to some extent under the “fair dealing” provisions in Chapter III of the Copyright, Designs and Patents Act from 1988. The “Consultation Paper on UK Implementation of the EC Directive” (accessible at <http://www.patent.gov.uk/about/consultations/eccopyright/>) does so far not contain any hint as to how the “fair compensation” requirement will be implemented.

First, it is regrettable that the Directive remains fairly vague in its wording on the relevant aspects of private copying, fair compensation and taking account of TPM. It “hides” a number of valuable pointers to its objectives in the Recitals, which serve as mere interpretative guidelines, but do not have binding authority, as does the text of the Directive itself. Clearer instructions to Member States in the body of the Directive would have been desirable, but the genesis of the Directive shows that an agreement on more precise language could not be reached. Therefore, the Directive has opted for harmonization at a minimum level for private copying. This offers Member States broad discretion on whether, or how, to shape this copyright exception. But it also shifts the problem of how to counterbalance competing interests to the Member States. The only clear and binding guideline given in Article 5, Para. 2, lit. (b) of the Directive on compensation for private copying is that the application or non-application of TPM *must* be taken into account when fixing “fair compensation”.

The wording inhibits a quick change away from the collective system of copyright levies towards individual licensing facilitated and administered by DRM. It will depend on the actual application, not the mere *availability* of TPM, whether or not tariffs compensating rightsholders must be assessed by taking TPM into account. For this reason, TPM must in fact be applied by the content industry and will probably need to reach a certain frequency and importance before they have a real impact on the collective copyright levy system. It must be kept in mind that there is no *obligation* for rightsholders to use copy protection measures or other DRM, as has been confirmed by the no-mandate provision of the Directive in Recital (48).¹³⁶⁷ Under German copyright law principles, it will also be difficult to argue that those content owners who do not lock-up their content through TPM tacitly agree to the copying of their works inside or outside the scope of the Private Copying Exception. This is because under German copyright law, rights are retained unless free-of-charge usage is explicitly granted. There is no such thing as an implied license by simply making copyrighted content available.

However, in the end, individual licensing, made possible through DRM, will be more attractive to the content industry than the traditional collective remuneration scheme through copyright levies, which only imprecisely reflects individual use of a work. At least, content owners who hold a strong market position and benefit from frequent use of their works will probably prefer individual licensing models. Eventually, DRM and the numerous prospects for copy control mechanisms offered to rightsholders can thus be expected to win recognition within the content industry. But the content industry will have to undertake joint efforts with the hardware industry to develop content which can be played on hardware, but not copied, if copy control mechanisms prevent such usage. In any case the copyright levy system and individual licensing through DRM will inevitably have

¹³⁶⁷ Recital (48) reads as follows: “[...] *Such legal protection implies no obligation to design devices, products, components or services to correspond to technological measures, so long as such device, product, component or service does not otherwise fall under the prohibition of Article 6. [...]*”.

to coexist for a transition period and this will also apply to digital use and digital copies. This is especially true since the Directive and the Copyright Bill only partially pave the way for a speedy acceptance of DRM.

Second, like the Directive, the Act deserves some criticism for its soft approach to private copying and the new requirements for the levy system. Germany has only partially accepted the Directive's objectives e.g., by the equal treatment of analogue and digital copies in the new Private Copying Exception Section 53, Para. 1 NGCA, although the Directive in Recital (38) expresses the wish that "[...] *due account should be taken of the differences between digital and analogue private copying and a distinction should be made in certain respects between them.*" The legislation did not follow the demands of the music and film industries to substantially restrict digital copying.

Third, the Act's re-enactment of the Directive's "fair compensation" principle and the duty to take into account the application of TPM is not satisfactory. Germany follows the duty to take TPM into account for "fair compensation" only by obliging the Copyright Collecting Societies to do so. Thus, in future the Copyright Collecting Societies will still be entitled to set up their tariffs irrespective of economic parameters and without being instructed how, in practice, they are to take TPM into account. They have in the past rightly been praised for their efficiency in representing the interests of rightsholders, but now it remains to be seen whether they are also flexible enough to take the next step to the digital age. This will involve not slowing down the development of TPM and individual licensing. But since a reduction of tariffs for digital copying would cut back their revenues, it is likely that they will be reluctant to take that step. According to the new Section 13, Para. 4 of the Copyright Administration Act, it lies within their power to introduce a flexible and fair tariff scheme. As announced by the German government, subsequent legislation will soon introduce a reform of the copyright remuneration scheme and tackle the difficult issue of Article 6, Para. 4, Subparagraph 2 of the Directive. It is desirable that as soon as possible the responsibility imposed by the Directive is accepted by regulating in more detail the copyright levy system to conform with the Directive's objectives.

Fourth, as an overall assessment, it remains to be seen whether the New German Copyright Act will pass the "reality test" and stop the sell-out of intellectual property through digital private copying. It also remains to be seen whether it will create enough incentive for the industry to continue developing practical and reliable DRM, given that the relatively "weak" mandate might not be an efficient means to implement the requirements of the Directive.

Thus, DRM, specifically their sub-category TPM, are continued to be treated with some suspicion. The Copyright Bill does not yet recognize TPM as a full and working alternative to the longstanding collective remuneration system through copyright levies. Copyright levies will not disappear in the near future. For the analogue use of copyrighted works and for copying of all content which has been published and distributed without copy protection throughout the last decades they will remain the only feasible way to ensure fair compensation of the rightsholder. Regarding digital use, however, copyright levies and their tariff system

must in the future become much more differentiated, both as to applicability and level. They must also distinguish between different types of equipment, depending on whether the equipment allows private copying or recognizes DRM. Already the new DVD+RW standard introduced by a number of market leaders in the computer hardware, electronic equipment and storage media industries recognizes copy protection measures which are integrated with the DVD media.¹³⁶⁸ Once equipment and blank media are interacting smoothly with the DRM used by the content industry, so that unauthorized copying is prevented, there is no longer a legal basis for paying copyright levies pursuant to Section 54 GCA. Under German law, it must also be kept in mind that a replacement of the levy system by individual remuneration through DRM must observe the standards of German data protection law. This could mean that remuneration can only be lawfully based on either anonymous or statistical data relating to the use of a work, but not on individual user data.¹³⁶⁹ This will give rise to new problems.

Neither the Directive nor the Act have provided final solutions to the relationship between private copying and DRM. For the content industry, the Copyright Collecting Societies and those developing DRM solutions the search for meaningful answers to the practical and legal challenges has only just begun.

¹³⁶⁸ For further details on the “DVD+RW Alliance” and technical information on DVD+RW and its interaction with DRM see <http://www.dvdrw.com>, last visited March 18, 2003.

¹³⁶⁹ See page 229 of the Data Protection Report 2003 by the Data Protection Officer for Northrhine Westfalia, accessible at <http://www.lfd.nrw.de/pressestelle/download/dsb2003.pdf>, last visited March 21, 2003.

4.3.3 Implementation of the European Info Directive in German Law and Its Consequences for Teaching and Research

*Bettina Böhm*¹³⁷⁰

In accordance with Article 5, Section 1, of the German Constitution (Grundgesetz), access to knowledge to participate in the scientific findings of others and to share this information with other researchers or students is an essential condition for research and teaching. In view of the extensive usage of electronic, especially net-based information and communication media at universities not only for research cooperation or distance learning but also in traditional “face-to-face” teaching, the question to what extent access to electronic works will be guaranteed in the future is critical.

At present, the Council Directive 2001/29 EC of the European Parliament and the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society which is supposed to adapt copyright laws to the developments in digital technologies, is at the centre of the discussion. The Law Governing the Copyright in the Information Society passed by the German Parliament on 11 April 2003 will implement significant parts of this Directive.¹³⁷¹ This amendment of the copyright law is likely to have noticeable consequences for the work of researchers, students and university services in the area of information, communication and media. Nevertheless, universities have so far been very reticent with regard to their participation in the legislative procedure and have, with some exceptions,¹³⁷² not actively expressed their position. Even the rather aggressive publicity campaign on the part of publishers, especially the German Booksellers and Publishers Association has had not changed this rather passive attitude.¹³⁷³

The copyright law is not easily accessible even for lawyers and thus even more complex for laypersons and it is not surprising that a broad discussion on this law and its amendment develops very slowly at universities. More importantly, present copyright laws have so far presented only few noticeable restrictions for everyday work at universities. Of course there have been certain uses of works

¹³⁷⁰ Universität Dortmund.

¹³⁷¹ See: Gesetzesentwurf “Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft”, BT Dr. 271/03, 02.05.2003.

¹³⁷² See the letter of the President of the Association of Universities and other Higher Education Institutions in Germany (HRK) to the Ministry of Justice of 23 October 2002, the joint declaration of the “Bundesvereinigung Deutscher Bibliotheksverbände e.V.” and the “Deutscher Bibliotheksverband” of 06 September 2002, and the statement of the “Deutsche Initiative für Netzwerkinformation e.V. (DINI)” of 28 November 2002. Detailed evaluation of the Draft Act can also be found in the statement of the “Institut für Rechtsfragen der freien und Open Source Software (ifrOSS)” of 11 December 2002.

¹³⁷³ See the letter of the President of the Association of Universities and other Higher Education Institutions in Germany (HRK) of 28 March 2003.

which have incurred claims from collecting societies in the past. University libraries, especially, had to negotiate licenses and fees for their on-demand services. For the most part, however, for university research, the past years have been characterized by a continuous expansion in the area of information and communication and thus also by an ever-expanding availability of works of third parties.

The amendment of the copyright law will now result in fundamental changes. In the future, it will not be the holders of the copyright or exploitation rights who will have to safeguard their claims for injunction or compensation. Rather, it will be the potential user who will have to gain access to the protected work. At that time, when resources which are today routinely used will not only be protected by legal provisions but actually be made inaccessible through technical measures,¹³⁷⁴ the copyright question will become a major question also for the day-to-day operations of universities and other institutions of research and learning. In addition to the so-called limitations which define the users' rights in research and teaching, the regulations on technical protection measures will receive special attention.

This contribution will discuss the question whether the amended law seems adequate to the needs of research and teaching, especially with regard to the limitations of the copyright law in the new § 52 a UrhG¹³⁷⁵ and the instruments for the enforcement of these limitations. In addition to a brief look at recent developments in U.S. legislation relating to distance education¹³⁷⁶, the potentially changing role of universities with regard to the questions of copyright will be addressed.

I Access to Electronically Available Works for Research and Teaching

As stated initially, the work of researchers depends on the unimpeded use of information in order to base their own research on this information and to share it with third parties. The amended law recognizes this need in § 52 a UrhG by permitting the use of published works in teaching¹³⁷⁷ or by making it available for a certain defined group of individuals for their own scientific research.

The question of whether the limitations defined in § 52 a UrhG establish an appropriate balance between the interests of research with regard to the use of electronically available works and the interests of copyright holders and publish-

¹³⁷⁴ For questions of the intertwining protection by technology, contracts and regulations, see: Auer-Reinsdorff, Brandenburg (2003): p. 155 et seq.; Bechtold (2002): p. 142 et seq., 249 et seq., 263 et seq.; Schack (2001): p. 221 n. 481b.

¹³⁷⁵ German Copyright Act.

¹³⁷⁶ Sec. 13301. Educational Use Copyright Exemption. Short Title "Technology, Education, and Copyright Harmonization Act (TEACH Act)" of 02 November 2002.

¹³⁷⁷ In the legislative proceedings the regulation has been clarified in the sense that it comprises teaching at schools *and universities*.

ers with regard to the exploitation of their rights¹³⁷⁸ will be asked from three different perspectives: with regard to the extent of the limitations, with regard to compensation, and with regard to the enforcement of these rights. In any case, the German Parliament has chosen a rather unusual procedure by setting a time limit to § 52 a UrhG which, according to § 137 k UrhG, only applies until 31 December 2006.

I.1 Extent of Limitations

§ 52 a UrhG regulates the collective use of works. Similar to the collective use of printed works, such as in a university seminar, the collective use of digitized works should be facilitated for certain groups of users. This limitation in § 52 a UrhG corresponds to the new § 19 a UrhG regulating the right of the author to make available a digitized work for the use by third parties independent of place and time.¹³⁷⁹

The regulation contained in § 52 a UrhG has proven to be highly controversial in the legislative proceedings. Critics of the regulation have warned of a threatened expropriation of publishers and authors: In the future, on-demand services would have the right to digitize and disseminate any protected work without authorization on the part of copyright holder. Soon there would be no library which would subscribe to scientific journals.¹³⁸⁰ This sharp criticism of § 52 a UrhG becomes plausible when considering the nature of digitized copies which, in contrast to analogue copies, can be passed on to an almost unlimited number of users without loss of time or quality.¹³⁸¹ On the other hand, these arguments are not entirely convincing. Right from the start, § 52 a UrhG was not meant as a general authorization for digitization and global dissemination of works in the area of teaching and research. Rather, it is a continuation of the rights defined in § 53 UrhG regulating individual copying for personal use in research and teaching. Individual copying by members of a particular research project or a particular class is thus replaced by making available a digitized version which can be used by this very same group.¹³⁸² In particular, § 52 a UrhG was never meant to allow dissemination of works by internet. Privileged use under § 52 a UrhG always requires a clearly defined group of users; in university teaching especially virtual classrooms with clearly defined access rights will meet these requirements.

One consequence of the strong resistance to § 52 a UrhG was the restriction of the regulation to small parts of a work, works of smaller scope or individual contributions from newspapers or journals. Apart from the fact that a partial use is not feasible for certain types of work (e.g. photographs, maps, technical

¹³⁷⁸ Which is also a question of establishing an appropriate balance with regard to the economic interests involved, see: Wandtke (2002): 6.

¹³⁷⁹ See: Auer-Reinsdorff, Brandenburg (2003): 53 et seq.

¹³⁸⁰ See: FAZ of 29 January 2003, n. 24, p. 1 "Enteignung der Autoren und Verlage?".

¹³⁸¹ See: Bechtold (2002): 251; Stopper (2002): 207 et seq; Wandtke (2002): 9.

¹³⁸² See: Stopper (2002): 214 et seq.

drawings),¹³⁸³ this restriction affects basic principles of scientific research and teaching.

In research groups, the collective use of works will hardly focus on one particular section of a work. Much more frequently, participating researchers will have to be provided with a broad spectrum of information which they will examine as to its relevancy for their research. A preliminary selection of information on the part of the provider is hardly compatible with this process.

In teaching, it is one of the obligations of an instructor to prepare students for independent evaluation of a variety of scientific methods and opinions. Especially virtual classrooms where instructors deposit materials for their classes provide opportunities to place the results of one's own research and one's own opinions into the context of other views and presentations. From the point of view of pedagogy, it does not seem adequate to furnish students with passages which are considered relevant rather than provide an opportunity for students to identify these important passages for themselves. Therefore, it remains to be seen if § 52 a UrhG will in fact support these new forms of teaching and learning.

The arguments against preliminary selection of information are even more valid when considering that the university as such, rather than the individual researcher and teacher, may act as information provider for the university community through intranet services. In this sense, central services of university libraries or media centres have been considered as privileged under the new legislation as long as the group of users is clearly defined and access is restricted by technical measures.¹³⁸⁴ In view of the controversial discussion of § 52 a UrhG in the course of the legislative proceedings, however, it is questionable whether the regulation covers such services at all.

The general exclusion of filmic works demanded by the critics would have significantly hindered scientific research, both in terms of media studies and because TV programs are often the only, or at least a necessary, source of information for current developments. According to the amended law, filmic works may not be used in research and teaching until two years after their release in the cinema. Given the relatively limited dangers for the film industry, this clause is not entirely plausible but will also not substantially hinder the use of these works.

I.2 Compensation

§ 52 a UrhG requires fair compensation for the right to make available copy-righted works.

A right to compensation appears entirely appropriate, balancing the interests of authors and users in the area of academic research.¹³⁸⁵ A closer look at the use of electronic works in research and teaching, however, reveals the difficulties

¹³⁸³ See the statement of the "Institut für Rechtsfragen der freien und Open Source Software (ifrOSS)" of 11 December 2002, p. 9.

¹³⁸⁴ See Hoeren in his statement "Was bleibt von der Wissenschaftsfreiheit — Überlegungen zu § 52 a des Entwurfes eines Gesetzes zur Regelung des Urheberrechts in der Informationsgesellschaft" of 17 October 2002, p. 5.

of realizing this approach. Established academic standards require the initial consultation of a large number of works. In the course of further research, a major portion will normally be excluded as irrelevant. If compensation is due right at the point of access rather than for actual use in a more specific sense, this might hinder academic work.

As long as § 52 a UrhG does not require an individualized right to compensation, but collective licenses, which must be managed by a collecting society, the question of compensation will not pose too many problems for researchers. Much more problematical are systems where rightholders or collecting societies claim fees which depend on the volume of *actual use* of the works made available. Both the technical instruments discussed in the next section and the announcement that the passed law will soon be amended by additional regulations, especially with regard to a future system of compensation, suggest that such a development is entirely probable.¹³⁸⁶

I.3 Enforcement of Limitations

The limitations provided for in § 52 a UrhG must also be evaluated as to their place in the overall conception of the new copyright law, in particular with regard to the new provisions in § 95 a and § 95 b UrhG.

As stated above, the amendment of the UrhG provides for a fundamental change in that it will not be the authors and other rightholders who will have to safeguard their claims to injunction or compensation, but the potential user who will have to gain legal access to the protected work.¹³⁸⁷ From a legal point of view, this reversal is required by the “Protection of Technological Measures” included in article 6 of the European Directive and the § 95 a UrhG based on this requirement.

§ 95 a UrhG protects technological measures by which a rightholder prevents the unauthorized use of a work by third parties.¹³⁸⁸ This regulation thus complements and provides legal protection for technical developments, especially in DRM systems.¹³⁸⁹ Depending on the state of development of these technical measures, the possibility of the use of electronic works in research and teach-

¹³⁸⁵ See the statement of the “Institut für Rechtsfragen der freien und Open Source Software (ifrOSS)” of 11 December 2002, p. 8.

¹³⁸⁶ See: Bechtold (2002): 257.

¹³⁸⁷ See: Schack (2001): 221 n. 481 b.

¹³⁸⁸ Critics have pointed out that § 95 a UrhG protects even those technological measures that do not aim at protecting Copyrights in the first place but intend to restrict market access. In the discussion on the European Directive, the question was raised whether technological measures are even protected against circumvention in research contexts. In German Law, this question has been decided in favour of the universities: § 95 a UrhG does not protect the rightholder against a circumvention of technological measures as long as this circumvention does not aim at breaching the Copyright.

¹³⁸⁹ See: Auer-Reinsdorff, Brandenburg (2003): 155 et seq.; Bechtold (2002): 202.

ing will substantially depend on whether the new § 95 b UrhG actually ensures access to electronic works as provided for by § 52 a UrhG.

§ 95 b UrhG requires the rightholder to furnish the user with the means required to make use of his rights but does not specify these means. According to the legal explanations, the access key may be provided for the individual user for single or multiple access or for organizations for autonomous distribution to entitled individual users.¹³⁹⁰ If researchers were forced to obtain the access key prior to each consultation of a particular work, the specific character of scientific research referred to above would be disregarded and the delays connected therewith would not be acceptable. Solutions, where central services such as libraries and media centres receive the necessary access key and, in turn, are obligated to protect the limitations seem more acceptable.

It is important to emphasize that § 95 b UrhG leaves it primarily up to the rightholders to decide how they comply with their obligation to provide the access key. § 95 b sec. 2 UrhG even implements a reversal of the burden of proof in favour of the rightholder: If the rightholder and the user have concluded an agreement specifying the means, the legal assumption is that these means are appropriate.

Moreover, the legal obligations of the rightholder according to § 95 b UrhG do not apply where special licensing contracts have been concluded with the user. Where access to electronically available works is provided, for example between the providers of digital magazines and university libraries, this is the rule rather than the exception.¹³⁹¹ In such cases, extent of and conditions for the use of digital works by researchers is thus less a question of legal regulations than of negotiating appropriate contracts.¹³⁹²

II Copyright Management at Universities

In connection with § 95 b UrhG, the possibility has been addressed that institutions of higher learning and media centres may receive the access key required and become in turn responsible for complying with copyright limitations. Corresponding new tasks for universities can also be found in the TEACH act which has come into effect in the United States in 2002.¹³⁹³

The introduction of Section 110 (1) (“Right to display and perform others’ work in the classroom”) into the Copyright Act of 1976 provides for an almost unlimited use of protected works for face-to-face teaching at U.S. universities. For distance education according to Section 110 (2), however, there have so far been

¹³⁹⁰ See the Draft Act, BT-Dr. 15/38 of 6 November 2002, p. 27.

¹³⁹¹ This also corresponds with the principles of the European Directive, see: Spindler (2002): 113.

¹³⁹² See: Bechtold (2002): 167, 258 et seq., 263 et seq; Schack (2001): 221 n. 481 b.

¹³⁹³ Sec. 13301. Educational Use Copyright Exemption. Short Title “Technology, Education, and Copyright Harmonization Act (TEACH Act)” of 02 November 2002.

significant limitations. The TEACH Act reduces the differences between face-to-face and distance education with regard to copyright although it provides for significant new obligations when using digital works within the framework of distance education:

The (accredited nonprofit) institution must institute policies regarding copyright that specify the standards educators will follow when incorporating copyrighted works into distance education. It must provide informational materials that accurately describe, and promote compliance with, the laws of United States relating to copyright. These materials must be provided to faculty, students, and relevant staff members. The institution must provide notice to students that materials used in connection with the course may be subject to copyright protection. In order to limit the transmission of content to students enrolled in the particular course the institution will have to apply technical measures that permit access only by students registered for that specific class and only for a specific period of time.

Even though the additional obligations arising from the TEACH Act, especially with regard to the selection of the sections of the works used, concern primarily the instructors themselves, the increased liability of the university as an institution may lead to the centralization of the design and use of distance learning in higher education.

At German universities, e-learning modules have so far been developed and used by individual researchers or smaller units such as departments. In the future, the universities as a whole may well incur obligations similar to their counterparts in the United States. Universities will have to develop appropriate frameworks for the implementation of DRM systems and licensing contracts in order to protect the rights of authors and publishers. These new structures are not exclusively protective mechanisms benefiting third parties. In the future, the development of tools and e-learning modules will have to be accompanied much more consistently by copyright management. Already in the early, conceptual phase, the necessary authorizations of third parties will have to be procured. Prior to the development of new teaching materials, the questions of newly emerging copyrights will have to be clarified and, with a view to the intended use, appropriate agreements will have to be drawn up between the parties involved.¹³⁹⁴

III Closing Remarks

It is assumed that universities in the near future will have to deal with questions of copyright far more frequently than today. Although the new § 52 a UrhG meets the demands of teaching and research at least to some extent, access to digitized works will probably be more difficult due to new instruments in legal and technical copyright protection. Any future system of compensation and any system of making available access keys in the sense of § 95 b UrhG that will force researchers to enforce their right to access prior to each consultation

¹³⁹⁴ See: Dusch, Sprenger (2003).

of a particular work will be hardly compatible with the specific character and needs of scientific research. Therefore, universities will have to provide organizational structures and technical measures that, on the one hand, allow teachers, researchers, and students easy access to digitized works and that, on the other hand, are acceptable in the view of rightholders with regard to their interests in protection and fair compensation.

4.3.4 New Copyright for the Digital Age: Political Conflicts in Germany

*Dirk Günnewig*¹³⁹⁵

Abstract: Based upon a found understanding, Digital Rights Management Systems (DRM) consist, particularly in the Business-to-Consumer commerce environment, of three interlocking components: technology, law and economics. Due to their integration into a social environment, several conflicts of interests arise that accompany the legal design of DRM systems. This article focuses on these conflicts using the example of the integration of the European Copyright Directive into the German Copyright Act. It thereby considers the interests, from a policy-analytical perspective, of the parties actively involved, the concrete areas of conflict as well as the resulting effects on political decision-making processes and real-world implementations. The primary intention is to provide the reader with an overview of the interests of the parties actively involved.¹³⁹⁶

I Introduction

The adaptation of the copyright law to the challenges of the digital technology showed particularly one thing: It was partly accompanied by profound conflicts of interests. This could be seen on international level at the World Intellectual Property Organization (WIPO), on supranational level at the institutions of the European Union (EU) or on national level e.g. in the USA or in Germany.

The existing legal framework can only cope in parts with the new challenges which the digitization to Intellectual Property (IP) causes. Unless it is able to regulate these challenges, resulting problems and conflicts of interest will occur, whose negotiation will be put on the policy agenda. On the one hand, matters will be settled in court and on the other hand within a law making process. Both can be considered as longterm and highly complex processes trying to re-define the final technology design and usage contracts, which are provided by the right holders.

Without modifications, a detailed reproduction of the balance of interests of the copyright in the legal scope fails for several reasons, namely:

1. The guarantee of copyright exemptions in DRM-systems is technologically problematic.
2. Legal digital distributions channels have to compete with illegal ones.
3. Problem of law enforcement.
4. The DRM-system enables new forms of dealing with IP.
5. The parties involved use the confrontation of the established balance of interests with the technological innovation to assert their interests again or for the first time.

¹³⁹⁵ Universität Dortmund.

¹³⁹⁶ Note: Only the statements of parties involved and political conflicts regarding the topic of this article could be taken into account as far as they were published until June 26th 2003. Only those statements are considered which are containing new information. Many of them only repeat prior statements.

6. Additional parties are affected by the regulation of the usage of DRM-systems and the effects of other instruments for (financial) compensation of the right holders in the digital area.

to 1) This aspect will be covered in chapter III.3.

to 2, 3) Problems in the area of digital IP are: Illegal distribution channels are or could be used by consumers who are not satisfied with legal offers of digital music, texts and movies and their conditions of usage. This illegal alternative exists because the same contents of legal offers are also available in illegal digital distribution channels (“Darknet”).¹³⁹⁷ At the same time, law enforcement is very difficult. There are two sources where illegal distribution channels get their content: First of all the content which existed before copy protection and DRM-systems were used. Second is the circumvention of technological protection measures of existing DRM- and copy-protection-systems. The technological protection of the content and the according usage conditions can be broken. This is proved by several examples. One is the circumvention of the Microsoft Media Player by a hacker with the pseudonym Beale Screamer.¹³⁹⁸ This is still and will be possible until the Internet and the end devices can be modified in a way that only such content can be used which is DRM protected or which digital format is certified by the right holders. In this scenario of such an environment other content could not be used.¹³⁹⁹

to 4, 5) According to the digitalization of content and the development of the ICT-infrastructure, a modification of the achievement of special components of the copyright law can be seen. At the same time the political principles regarding the balance of interests are unchanged.¹⁴⁰⁰ These principles as well as the interests of the right holders, guarantee access by society. A turning away from these principles is not expected especially because it is socially based and formalised by law. Even if this two principal aims could be transferred into the “*digital age*”, it is not possible to realise a precise transformation of the balance of interests established in the non-digital area into the digital age. This is not possible according to the statements dealt with below.

With the application of DRM-systems additional conflict will arise: Existing forms of the management of digital IP are replaced. One example is the discussion on the issue of the remuneration of copyright exemptions as levies to the right holders. It is discussed if the existing system of collective and

¹³⁹⁷ See: *Biddle, England, Peinado, Willman* within this book (page 344).

¹³⁹⁸ See: Screamer (2001). See also: *Hauser, Wenz* within this book on page 206.

¹³⁹⁹ See: Plura (2002): 186; *Kuhlmann, Gehring* within this book on page 178. Note: In this environment it is also still questionable if the principal security risk of digital IT-systems could be eliminated. This known principal security risk is that all systems can be broken sooner or later. Furthermore older devices and older software could be used which are not modified in this special way.

¹⁴⁰⁰ See: Committee on Intellectual Property Rights and the Emerging Information Infrastructure (2000): 11.

flat rate remuneration and the charging of devices and blank media could be replaced by an individual remuneration system enabled by DRM-systems. New problems and new challenges for the problem solving systems of the policy field are resulting from the application of the technological innovation. One of those is the possibility of data mining and creating user profiles which are considered as data protection and privacy problems.

Discussions about the established balance of interests regarding to the usage of digital IP in the society do not mean that every party agrees. Democracies create consensus among the various parties concerned by its regulation. But this should not disregard the fact, that the actors do not see their interests adequately represented in the legal framework. They work toward influencing the legal framework according to their interests. A new situation due to technological innovations and their effects on the economic situation and the legal framework is a welcome opportunity. With these discussions new problems arise and “old” issues are revived.

The interest groups try to influence the copyright law according to their own interests. One example for that is the German IFPI¹⁴⁰¹ demanding the abolition of the copyright exemption for private copying.

DRM-systems are therefore used as an argument to alter the existing copyright system. One example is the lobbying efforts of the ICT-industries, which aims at establishing a system for the remuneration of copyright exemptions based on individual payments for the usage of these exemptions. In this way the existing system of collective and flat rate remuneration should be removed, which leads to the removal of levies on ICT like scanners or CD-burners which have to be paid by ICT-industries.

to 6) “One could rely on the ‘implied consent’ of the classic copyright circle whose members have known each other for decades. They also met in the same circles and made political decisions in the area of copyright law beforehand in smaller ‘family circles.’”¹⁴⁰² — this is how Hoeren described the course of political conflicts of interests in the copyright area until the end of the seventies. This „closed shop“ became more open as a result of the IP digitalization.

Today new parties try influencing the political decision making processes to suit their interests. The German ICT-industry is, one of those actors in the policy field, highly affected by the intended amendment of German copyright law. These companies see themselves having to pay additional millions in copyright levies on ICT-technologies.

For this article only some paragraphs of the drafts of the amendment of the German Copyright Act (Urheberrechtsgesetz, UrhG) are relevant; only those which

¹⁴⁰¹ German Group of the International Federation of the Phonographic Industry.

¹⁴⁰² See: Hoeren (2002): 108. German original: “Man konnte sich dabei bislang auf den ‘implied consent’ der klassischen Urheberrechtskreise verlassen, die einander über Jahrzehnte kannten, sich in den stets gleichen Zirkeln trafen und rechtspolitische Entscheidungen vorab im kleinen Kreis der ‘Familie’ trafen.”

deal with DRM–systems or copyright exemption and the future remuneration system for digital private copying.

Based on the analysis of the statements by the parties involved on the draft for a bill amending the German Copyright Act, the following fields of conflict are identified:

Major conflicts of interests	Minor conflicts of interests
Legitimacy of the application of copyright exemptions in the digital area	Limitation of the legal protection against the circumvention of technical measures in favour of copyright exemptions
	Limitation of usage contracts in favour of copyright exemptions
Individual vs. flat rate (collective) remuneration of copyright exemption	Evaluation of the flat rate (collective) remuneration system for the digital area
	Evaluation of the individual remuneration system enabled by DRM–systems
	Evaluation of the technological status quo of DRM–systems
	Legal protection against circumvention of technical measures
	Privacy

Tab. 1. Conflicts Regarding the Application of DRM–Systems

Fig. 1 refers to fundamental questions which are to be discussed by the parties involved. The question is fundamental, if a usage in accordance to the copyright exemptions should be allowed or not. If it is not, it would not be necessary to think about the possibility of changing the system of the compensation of these exemptions.

The following statements in this article relate only to the parties listed in the following chapter. According to the possible sources of information and the large amount of written and other statements, campaigns, websites, press releases, articles in the media and the statements of representatives of the interest groups at hearings and conferences a restriction has to be made. Therefore parties and pressure groups involved could partly modify their position. As a consequence their interests can not be considered exactly. Furthermore the interests have perhaps been discussed in formal or informal meetings with political decision makers and the ministerial bureaucracy.

In the following chapters of this article, some generalizations were necessary. Therefore not every nuance of the political statements of the lobby–groups can be described because clarity and evaluation would suffer. Instead it is the aim to describe the interests according to those observed by the author. In parts the nuances of the interests are explained in the footnotes. The evaluation of

the final implementation of the German Copyright Act of the parties involved will also not be considered. Instead only the interests which have been voiced in the decision making process will be taken into account. This will be part of the dissertation on political science written by the author published in 2004.

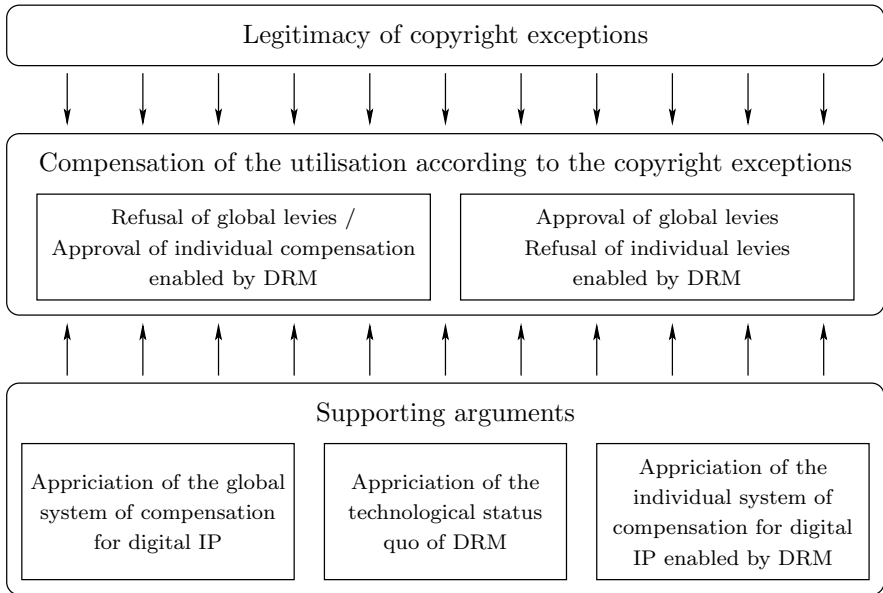


Fig. 1. Conflict Areas

This article refers to the description of the legal framework of the collective and individual remuneration system which has already been discussed in the articles by *Dreier* and *Nolte* (page 479), *Ulmer–Eilfort* (page 447) and *Goldmann* (page 502) and by *Lejeune*, *Reinbothe*, *Bygrave*, *Dusollier*, *Böhme*, *Hoeren* and *Bechtold* in regard of the legal framework (and conflicts) on which the conflicts of interests rely.

II Parties Involved and the Structure of the Policy Field

Federal policies are not only the result of the politics of the government or the parliament but also come from strategic interaction of various parties with a variety of different interests and motivations.¹⁴⁰³

A large number of various parties — approx. 100 — are affected by the amendment of the copyright law. Only 35 of them are actors concerned about the conflicts regarding the usage of DRM–systems and the digitalization of IP.¹⁴⁰⁴

¹⁴⁰³ See: Scharpf (2000): 34; Schneider (2003): 107.

These 35 political actors can be categorised in the following classes: creators/authors, content providers, users (corporate, commercial users and end-users).

The definition of the *group of the creators* of intellectual property (IP) is very problematic because of its heterogeneous structure. A systematisation could be done according to various artificial expressions — text, movie and music — or to functions — authors, performing artists, journalists, composers, poets etc.¹⁴⁰⁵

The “associations of creators” have also been taken into account: Bundesverband Kamera (BvKamera)¹⁴⁰⁶, Deutscher Journalisten-Verband (DJV)¹⁴⁰⁷ and ver.di Fachbereich 8 Medien, Kunst und Industrie (verdi) (former Industriegewerkschaft Medien (IG Medien)¹⁴⁰⁸). It seems that the range of the “artists” is underrepresented due to the definition above. Looking at the main organisation of journalists, verdi, it can be seen that there is a sub-group of approx. 6000 authors and musicians.¹⁴⁰⁹ Only a few artists gave their comments.¹⁴¹⁰

The *content providers* are divided in media forms like text, music, film and multimedia. They are well organized by a professional structure of associations: in the publishing business by the Börsenverein des deutschen Buchhandels (Börsenverein)¹⁴¹¹ and the VdS Bildungsmedien (VdS)¹⁴¹², Bundesverband Deutscher Zeitungsverleger (BDZV)¹⁴¹³ and Verband Deutscher Zeitschriftenverleger (VDZ)¹⁴¹⁴.

¹⁴⁰⁴ Note: Only the interests of those parties are considered who refer their statements in direct or indirect connection to DRM systems and their effects on copyright in the digital age. They are taken into account if their statements refer to relevant parts of the implementation of the directive 2001/29/EC (below copyright directive). Furthermore those parties are not taken into consideration who do not show significant distinctions to the statements and interests of those pressure groups and central association in which they are organized themselves.

¹⁴⁰⁵ A detailed description of the considered parties of the policy field is not provided in this article, but will be published in the current dissertation being undertaken by the author.

¹⁴⁰⁶ Note: German Association of Cinematographers. The BvKamera is a association of camera men defining the profession. See: <http://www.bvkamera.org>

¹⁴⁰⁷ Note: Association of journalists. See <http://www.djv.de>

¹⁴⁰⁸ Note: Trade union with members ranging from journalists to artists and authors. See http://www.verdi.de/fachbereiche/medien_kunst_industrie

¹⁴⁰⁹ See: verdi (2002).

¹⁴¹⁰ Note: Smudo — Michael B. Schmidt — owner of the record label “*Four Music*” and member of the “*Die Fantastischen Vier*” (German music group) gave interviews (See: Friebel (2000); Smudo (2000).) and lectured on conferences (e.g. workshop on DRM in November 2000. See: <http://www.digital-rights-management.de>) to present his view.

¹⁴¹¹ Note: Association of publishers and book sellers. <http://www.boersenverein.de/>

¹⁴¹² Note: The VdS Education Media has a similar focus like the Börsenverein but they represent the publishers and sellers of educational media. Website: <http://www.vds-bildungsmedien.de/html/vds.htm>

¹⁴¹³ Note: Association of newspaper publishers. See <http://www.bdzv.de/>

¹⁴¹⁴ Note: Association of German magazine publishers. See <http://www.vdz.de/>

Two associations of the music industry are taken into account: German Group of the International Federation of the Phonographic Industry (IFPI) / Bundesverband der phonographischen Wirtschaft¹⁴¹⁵ and Deutscher Musikverleger-Verband¹⁴¹⁶. The various parts of the movie industry are organized in a major association, the Spitzenorganisation der Deutschen Filmwirtschaft (SPIO).¹⁴¹⁷ The other relevant association, the film20 Interessengemeinschaft Filmproduktion¹⁴¹⁸ is not a member of SPIO. They published joint statements.

The *users* are the most heterogeneous group consisting of different parties, who use copyright protected contents in alternative ways. They are divided into commercial, corporate users and end-users (consumers).¹⁴¹⁹

ICT-industries are *commercial users*. They use copyright protected contents themselves or provide consumers with devices and blank media. They are profit organisation. The Branchenverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM)¹⁴²⁰, the Bundesverband der Deutschen Industrie (BDI)¹⁴²¹ and the Deutscher Industrie & Handelskammertag (DIHK)¹⁴²² are taken into account.

The *corporate, non-profit users* are either using the contents or enable consumers / end-users to use them. They are not profit orientated. The Allgemeine Deutsche Rundfunk (ARD), the Zweite Deutsche Fernsehen (ZDF)¹⁴²³ and the Bundesvereinigung Deutscher Bibliotheksverbände (BDB) / Deutscher Bibliotheksverband (BDV)¹⁴²⁴ and the Deutsche Gesellschaft für Informationswissenschaft und Informationspraxis e.V. (DGI)¹⁴²⁵ are considered in this context. In October 2002, the Hochschul Rektoren Konferenz (HRK) got involved by giv-

¹⁴¹⁵ Note: These two associations of the phonographic industry are working closely together, have a common branch and publish joint statements. See <http://www.ifpi.de/>

¹⁴¹⁶ Note: Association of German music publishers. The DMV is an association representing the interests of music publishers for almost 90% of all music publishers working in Germany. See <http://www.dmv-online.com/>

¹⁴¹⁷ Note: Association of the German movie industry. See <http://www.spio.de/>

¹⁴¹⁸ See <http://www.film20.de>

¹⁴¹⁹ Publishers are also users of contents, but they belong to the group of content providers because they have similar interests and perspectives like other parties of this group.

¹⁴²⁰ Note: German Association for Information Technology, Telecommunication and New Media. BITKOM represents companies in the information economy, telecommunications and the new media in Germany. See <http://www.bitkom.org/>

¹⁴²¹ Note: German Industry Association. See <http://www.bdi-online.de>

¹⁴²² Note: Association of German Chambers of Industry and Commerce. These Chambers represent the German industry and commerce with the exception of handicraft businesses, free professions and farms. Website: <http://www.dihk.de>

¹⁴²³ Note: TV-stations. Websites: <http://www.ard.de> and <http://www.zdf.de>

¹⁴²⁴ Note: Associations of public and non-profit libraries. See: <http://www.bdbverband.de> and <http://www.bibliotheksverband.de>

¹⁴²⁵ Note: The Association for Information Science and Practice. <http://www.dgd.de>

ing statements regarding the copyright exemption for education and research (§ 52a).¹⁴²⁶

Scientists, teachers, students and consumers belong to the *end-users*. Only a few parties of this group gave statements on the topic. The most important association of this group is the Bundesverband der Verbraucherzentralen und Verbraucherverbände.¹⁴²⁷ Also a private initiative, Initiative Privatkopie.net, was founded in April 2002. It is an alliance of scientists, media activists and their organisations.¹⁴²⁸ One criticism is that the end-users have no active lobby in the political decision making process.¹⁴²⁹

The *collecting societies* are one of the more important parties in policy field copyright. They are private associations aiming at fiduciary administration and collective award of remuneration rights for holders of copyright and related rights.¹⁴³⁰ Collecting societies also concede copyrights to users of the contents.¹⁴³¹

Out of the eleven German collecting societies, only the Gesellschaft für musikalische Aufführungs- und mechanischer Vervielfältigungsrechte (GEMA),¹⁴³² the VG Wort¹⁴³³, the VG Bild-Kunst¹⁴³⁴ and the Zentralstelle für private Überpielungsrechte (ZPÜ)¹⁴³⁵ are taken into account.

¹⁴²⁶ Note: The Hochschulrektorenkonferenz (HRK) is the voluntary association of state and state-recognised universities and other higher education institutions in Germany. It has currently 262 member institutions where approx. 98 per cent of all students in Germany are registered. See <http://www.hrk.de>

¹⁴²⁷ Note: Federation of German Consumer Organisations is engaged in lobby work for consumer interests and is the umbrella organisation of 37 German consumer associations. See <http://www.vzbv.de>

¹⁴²⁸ Note: In December 2002 they presented the Minister of Justice, Brigitte Zypries, with 35.000 “*virtual*” signatures demanding the right of private copying. See: Krempl (2002f). The library association “Deutscher Bibliotheksverband” asked the visitors of their website to support the petition of Privatkopie.net. See: DBV (2002). See <http://www.privatkopie.net>.

¹⁴²⁹ See: Wilkens, Zota (2002).

¹⁴³⁰ See: § 1 para. 1 and 4 UrhWahrnG. § 1. para. 1 i.V.m. para. 1 WahrnG. § 2 Satzung der GEMA. § 1 Satzung der VG Wort. § 2 Satzung der VG Bild-Kunst. [Note: The “Satzung” is the articles of association.] See also: Goldmann (2001): 1; Kreile, Becker (1997a): 664.

¹⁴³¹ See: Kreile, Becker (1997): 622; Bing (2001): 154.

¹⁴³² Note: German Society for Musical Performing and Mechanical Reproduction Rights. As a state-recognised trustee organisation, the GEMA administer the exploitation rights of creators of music as a collecting society. See <http://www.gema.de>

¹⁴³³ Note: Collecting society for lyrics and compositions. See <http://www.vgwort.de>

¹⁴³⁴ Note: Collecting society for photographs and paintings. See <http://www.bildkunst.de>

¹⁴³⁵ Note: Organisation for Private Recording Rights. The ZPÜ is a collection society for the eleven German collecting societies. It deals with levying and remuneration of the fees on devices and blank media for private copying. See <http://www.gema.de/kunden/zpue>

Some parties could not be assigned to one specific category because they are integrating several groups. One of them is the Forum der Rechteinhaber¹⁴³⁶. In this “Forum” various associations of the content providers like the Börsenverein or the IFPI and some collecting societies like the GEMA and the VG Bild–Kunst are organized. When the implementation of the EU Copyright Directive into German copyright occurred, the members published joint statements. Another is the Deutscher Kulturrat¹⁴³⁷ which members are authors and collecting societies.

III Legitimacy of Copyright Exemptions

The exclusive exploitation right of the author is limited¹⁴³⁸ because of the German constitution, which states, “Property obligates”.¹⁴³⁹ These copyright limitations are defined in the copyright exemptions. The permission of the free use of intellectual property according to the copyright exemptions has not to be mixed up with use free of charge. According to the exemptions regulations apart from the remuneration–free also remuneration–requiring uses exist. The permission of the free use means that it does not depend on the agreement and the conditions of the right holders. The user must pay a “fair compensation” to the right owner, if remuneration charging is present, usually this is financial.

For the technical design of DRM systems it is crucial whether copyright exemptions must be made possible according to certain uses. Furthermore it is important whether a compensation is to be realized by the DRM system. In Germany and some other continental–European states, two strategies are hit in order to guarantee financial reconciliation: On the one hand there is an individual right perception, assignment and remuneration and on the other hand there is a collective and flat–rate view on this.¹⁴⁴⁰ As far as possible for practical reasons, the individual method is used — also in the non–digital environment. In the individual right perception and assignment, the right owner determines the use conditions. Otherwise a collecting society is taken into the obligation.

¹⁴³⁶ Note: Forum of the right holders. The organisations involved are the Association of Publishers and Booksellers of Germany: German Federation of the Phonographic Industry, the German National Group of IFPI, the German Music Publishers’ Association, the VdS Education Media as well as the collecting societies GEMA, GVL, VG Wort, VG Bild–Kunst, GÜFA, GWFF, VFF and VGF united in ZPÜ (German Central Organisation for private Copying Rights). See: http://www.gema.de/kommunikation/pressemitteilungen/eu_info_richtlinie_pm.shtml

¹⁴³⁷ See <http://www.kulturrat.de>

¹⁴³⁸ See: §§ 15, 16, 17, 18, 19, 20, 21, 22 German Copyright Act (Urheberrechtsgesetz). Note: The exclusive right assures in other cases the personal regulation of use conditions for the intellectual property of the author to him. See: §§ 45, 46, 47, 48, 49, 50, 51, 52, 53 German Copyright Act. See article of *Ulmer–Eilfort* (page 447), *Goldmann* (page 502), *Dreier, Nolte* (page 479) within this book.

¹⁴³⁹ See: Art. 14 GG. German constitution (Grundgesetz); Hoeren (2001): 12.

¹⁴⁴⁰ See: Becker (2002); Goldmann (2001): 61.

The two strategies and the associated conflicts of interests are described in the following minor chapter.

The parties involved have first to deal with the following fundamental question:

1. Do copyright exemptions also apply within the digital area? If so, which?

If yes, further questions follow:

2. How does the compensation of uses according to the copyright exemptions take place as “fair reconciliation”?
3. Do copyright exemptions apply, if technical protection measures protect the intellectual property?
4. Do copyright exemptions apply, if “user contracts” for the IP between right owners and users are signed?
5. Which quality should the private copy have for example? (e.g. May the copy remain DRM protected? Is a reduced quality sufficient for the copy?)

Further questions follow, if technical protection measures protect IP: Can they enable copyright exemptions without losing their protection function? This is a complicated question as stated by Clark: “*Digital-rights management technology cannot simultaneously meet the desires of both copyright holders and consumers who desire to make ‘fair use’ of copyrighted material, a panel of technologists, lawyers and business officials here agreed during a session Tuesday evening.*”¹⁴⁴¹

Apart from these five questions it is discussed, whether copyright exemptions should be principally permissible, whether the IP is in a digital or an analog format.

In connection with the amendment of the German copyright — above all — the following two types of copyright exemptions are considered: private copying¹⁴⁴² and making available for education and research.¹⁴⁴³ The copyright exemption in favour of handicapped persons¹⁴⁴⁴ was not controversial and therefore it has not been considered in this article. The main issue of this chapter is the copyright exemption in favour of private copying. At it, the fundamental conflicts of interest regarding copyright exemption become clear.

III.1 Private Copying

The conflicts of interest regarding the future of the private copying within the digital area receives more public attention, than conflicts regarding other copyright exemptions. For example PC-magazines reported in detail on this group of topics. They describe instructions for the circumvention of copy protection mechanisms. Furthermore numerous consumers organized themselves, to fight for the perpetuation of digital private copying. They have collected approx. 40.000 ”virtual” signatures up to the end of April 2003.

¹⁴⁴¹ See: Clark (2002).

¹⁴⁴² See: § 53 copyright draft law (version 6/11/2002).

¹⁴⁴³ See: § 52a copyright draft law (ver. 6/11/2002).

¹⁴⁴⁴ See: § 45a copyright draft law (ver. 6/11/2002).

Three controversially judged core-questions exist regarding private copying:

1. approval or refusal of the digital private copy
2. approval or refusal of the making of private copies by a third person
3. approval or refusal that a legal source for making a private copying is needed

	Approval of the digital private copy	Refusal of the digital private copy
Authors	bvkamera ¹⁴⁴⁵	
Content providers	Börsenverein ¹⁴⁴⁶ BDZV ¹⁴⁴⁷	IFPI ¹⁴⁴⁸
Users	ARD, ZDF ¹⁴⁴⁹ BDB, DBV, DGI ¹⁴⁵⁰ DBV ¹⁴⁵¹ Privatkopie.net ¹⁴⁵² VZBV ¹⁴⁵³	
Collecting societies	GEMA ¹⁴⁵⁴ VG Bild-Kunst ¹⁴⁵⁵ VG Wort ¹⁴⁵⁶	
Others	Kulturrat ¹⁴⁵⁷	

Tab. 2. Copyright Exemption for Private Copying

The IFPI, who represents the music industry, opposes the digital private copying whilst endorsing the application of copy protection technology. Although it loses the source of income of the remuneration for private copies, making the private copy possible promotes the “piracy” according to the opinion of the music industry. “Piracy” is perceived as causing more losses for the industry, than the remuneration generated by private copying.¹⁴⁵⁷

This fits also the argumentation the GVV: Therefore the private copy would have almost as negative economic consequences for the industry as the illegal use of their contents. For the right owners it would make no financial difference whether

¹⁴⁴⁴ See: bvkamera (2002).

¹⁴⁴⁵ See: Heker (1998); BMJ (2000): 38.

¹⁴⁴⁶ See: BDZV (2001); BDZV (2002).

¹⁴⁴⁷ See: Schaefer (2000); BMJ (2000): 38; Röttgers (2001); See also: IFPI (2001); IFPI (2001a); Schaefer (2000); IFPI (2002a): 36.

¹⁴⁴⁸ See: ARD, ZDF (2002).

¹⁴⁴⁹ See: BDB, DBV, DGI (2002); Beger (2002).

¹⁴⁵⁰ See: DBV (2002).

¹⁴⁵¹ See: Initiative Privatkopie.net (2002).

¹⁴⁵² See: VZBV (2002); VZBV (2002a).

¹⁴⁵³ See: GEMA (2002); GEMA, VG Wort, VG Bild-Kunst (2002)

¹⁴⁵⁴ See: BMJ (2000): 38. VG Bild-Kunst (2002): 2.

¹⁴⁵⁵ See: BMJ (2000): 38

¹⁴⁵⁶ See: Kulturrat (2002); id. (2002a): 17; id. (2002b).

¹⁴⁵⁷ Note: The remuneration does not aim in compensating financial losses because of illegal copies but of usages according to the copyright exemptions.

100.000 illegal CDs flow on the German market, or whether 20.000 times five private copies are manufactured.¹⁴⁵⁸ According to German copyright the non-digital private copy has minimum impact.¹⁴⁵⁹ The digital private copy intervenes disproportionately strong in the primary utilization, as the associations of the content providers state.

The IFPI endorses the non-digital private copy in principle.¹⁴⁶⁰ However the association demands that each kind of private copy — digital or analog — depends on the permission of the right holder.¹⁴⁶¹ Similar interests represent the SPIO and film 20, who are representatives of the movie industry. Their position can not be specified on a clear endorsement or refusal of the digital private copy. They do not demand the fundamental abolishment of the digital private copy. Instead SPIO and film 20 endorse a gradated private copy for movies. Therefore visitors of cinemas would have no right to video-tape the movie. Buyer or borrower of copy-protected DVD would get no right to private copying. Private copies are only legitimate if a movie is transmitted on television.¹⁴⁶² The SPIO and film 20 judge this as a compromise between the interests of the industry represented by them and the consumers.

In the Copyright draft law the quality and extent of the digital private copy were not finally defined. Instead only the implementation-requiring components of the EU copyright directive are to be regulated in this first amendment of the German Copyright act.¹⁴⁶³ In accordance with the copyright draft law (ver. 6/11/2002) private copies can also be made by third persons — which must be free of charge.¹⁴⁶⁴ Only a few parties published statements on this issue. ARD and ZDF,¹⁴⁶⁵ VZBV,¹⁴⁶⁶ BDB and DGI¹⁴⁶⁷ are promoting this. BITKOM,¹⁴⁶⁸ BDI,¹⁴⁶⁹ VPRT¹⁴⁷⁰ (commercial users) and BDZV,¹⁴⁷¹

¹⁴⁵⁸ See: Schaefer (2000).

¹⁴⁵⁹ See: Bundestag (1997): 30.

¹⁴⁶⁰ Note: IFPI and “Bundesverband der phonographischen Wirtschaft” do not call the private copy in the non-digital area but in the digital area in question. The paragraphs 53 and 54 of the German Copyright Act should be unaltered and the collective and flat rate remuneration should be retained. See: IFPI, GEMA (2002).

¹⁴⁶¹ See: Schaefer (2000); BMJ (2000): 38; Röttgers (2001); Schaefer (2000); IFPI (2001); IFPI (2001a); IFPI (2002a): 36; IFPI (2002d).

¹⁴⁶² See: SPIO, Film 20 (2002c).

¹⁴⁶³ See: copyright draft law (ver. 6/11/2002) Begründung A. Allgemeiner Teil I. Ziel und Gegenstand. page 15. See also: Bundestag (2002). Note: Other questions concerning the private copy are shifted on a following second legislative procedure.

¹⁴⁶⁴ See: § 53. para. 1. copyright draft law (ver. 6/11/2002).

¹⁴⁶⁵ See: ARD, ZDF (2002): 1.

¹⁴⁶⁶ See: VZBV (2002).

¹⁴⁶⁷ See: Beger (2002).

¹⁴⁶⁸ See: BITKOM (2002e).

¹⁴⁶⁹ See: BDI (2002).

¹⁴⁷⁰ See: VPRT (2002a); VPRT (2002b): 2.

¹⁴⁷¹ See: BDZV (2002).

VDZ,¹⁴⁷² Forum der Rechteinhaber¹⁴⁷³ and GVU¹⁴⁷⁴ (content providers) and the political party CDU¹⁴⁷⁵ are rejecting it. The production of private copies by third persons would lead to the risk of abuse.¹⁴⁷⁶

III.2 Copyright Exemption for Education and Research

The copyright exemption for education and research (§ 52a Copyright draft law¹⁴⁷⁷) contains obviously enormous conflict potential. The Federal Ministry of Justice accomplished a special hearing regarding this copyright exemption. The parliamentary debates¹⁴⁷⁸ and the political debates in the public showed, that the § 52a was discussed very contentious.

	Refusal of § 52a copyright draft law	Approval of § 52a copyright draft law
Content providers	BITKOM, BDI, VDZ, BDZV, VdS ¹⁴⁷⁹ Börsenverein, VdS ¹⁴⁸⁰ SPIO / Film 20 ¹⁴⁸¹	
Users	BITKOM ¹⁴⁸²	BDB, DBV, DGI ¹⁴⁸³ HRK ¹⁴⁸⁴
Others	Forum der Rechteinhaber ¹⁴⁸⁵	

Tab. 3. Copyright Exemption for Education and Research

In particular the representatives of the content providers and the ICT industries criticize vehemently the appropriate paragraph of the draft law. The law leads to substantial economic disadvantages for the primary utilization of digital goods, explained representatives of the content providers like the VdS or the Börsenverein. VdS represents school book and educational medium publishing houses. These enterprises create contents for the circle of the beneficiaries of

¹⁴⁷² See: VDZ (2002a): 4.

¹⁴⁷³ See: Forum der Rechteinhaber (2002): 5; id. (2002b).

¹⁴⁷⁴ See: GVU, Tielke (2002); GVU, Scharringhausen (2002).

¹⁴⁷⁵ See: Krempl (2003).

¹⁴⁷⁶ See: VPRIT (2002a). Forum der Rechteinhaber (2002b).

¹⁴⁷⁷ See: Article by *Böhm* on the legal aspects of § 52a withinin this book (page 520).

¹⁴⁷⁸ See: Bundestag — Rechtsausschuss (2003).

¹⁴⁷⁹ See: BITKOM, BDI, VDZ, BDZV, VdS (2002)

¹⁴⁸⁰ See: VdS (2002a); VdS (2002); Börsenvereins, VdS (2002).

¹⁴⁸¹ See: SPIO, Film 20 (2002b): 3; id. (2002a): 4; id. (2002c).

¹⁴⁸² See: BITKOM (2001g).

¹⁴⁸³ See: Beger (2002); BDB, DBV, DGI (2002).

¹⁴⁸⁴ See: HRK, Landfried (2002). Note: The Hochschulrektorenkonferenz (HRK) is the voluntary association of state and state-recognised universities and other higher education institutions in Germany. It currently has 262 member institutions at which approx. 98 per cent of all students in Germany are registered.

¹⁴⁸⁵ See: Forum der Rechteinhaber (2002b).

this copyright exemption. Therefore the VdS and the Börsenverein — as well as BITKOM, BDI, VDZ and BDZV — demand the cancellation of the paragraph without substitution.¹⁴⁸⁶ The provision would endanger their means of existence. The VdS and the Börsenverein even accuses an obvious connection between the empty public education cash boxes and the legislative initiative to the Federal Government.¹⁴⁸⁷ The affected German publishers interpreted the provision of § 52a as a compulsory purchase of the publishers and authors.¹⁴⁸⁸ The Börsenverein criticized that the libraries would have to buy only one copy of a book or a magazine to make it available to all libraries in Germany.¹⁴⁸⁹ Just before the amendment of German Copyright law was adopted, one campaign of the Börsenverein and some publishers works for educational and scientific purposes attracted interest. In this campaign they repeated their fear according to § 52a.¹⁴⁹⁰ They published a campaign website which contains severe criticism which aims in the cancellation of § 52a.

This campaign aroused antinomy and criticism by the libraries and the Federal Ministry of Justice. The Federal Minister of Justice, Zypris, declined these predications. In connection of § 52 libraries would not be the object, she stated. The § 52a would only deal with research and education from the perspective of the recipients of the exemption like researchers, teachers or pupils. Zypris explained that the Copyright Draft Law would not permit libraries and schools to copy copyright protected works arbitrarily.¹⁴⁹¹ A similar argumentation could be found at the associations of public libraries and of universities. § 52a would not allow the libraries to digitalize complete library stocks which are made accessible to a indefinite circle of users. These associations stated that Börsenverein has supplied misinformation.¹⁴⁹²

In the opinion of critics, substantial constitutional doubts exist against the validity partial of a remuneration-free access to protected works. This copyright exemption would intervene in the property right of the right holders too strong.¹⁴⁹³ This creates a legal grey area, which endangers also the protection of technical measures. This is justified with the fact that in addition the technical protection system would probably have to be broken to enable the copyright exemption.

Critics describe the following scenario if the paragraph is valid: A school or a teacher could buy only one copy of a copyright protected content. They could

¹⁴⁸⁶ See: VdS (2002); VdS (2002a); BITKOM, BDI, VDZ, BDZV, VdS (2002).

¹⁴⁸⁷ See: VdS (2002a); Verlage und Wissenschaftler für ein faires Urheberrecht (2003)

¹⁴⁸⁸ See: Bundestag — Rechtsausschuss (2003).

¹⁴⁸⁹ See: Verlage und Wissenschaftler für ein faires Urheberrecht (2003).

¹⁴⁹⁰ See: VdS (2002a); Verlage und Wissenschaftler für ein faires Urheberrecht (2003a); id. (2003c); id. (2003); id. (2003d); id. (2003e).

¹⁴⁹¹ See: id. (2003). Article by *Böhm* within this book (page 520).

¹⁴⁹² See: HRK, Landfried (2003).

¹⁴⁹³ See: Forum der Rechteinhaber (2002b); VdS (2002); VdS (2002a); Kreutzer (2002).

scan it and afterwards they could spread it to the students without remunerating the right owners.¹⁴⁹⁴ This problem is also present at universities. At present they often purchased several copies of important contents for their libraries. This will no longer be necessary, because they can acquire a copy and make it available in the Intra-net.

Furthermore, it would be problematic to define, who belongs to the “defined circle of acquaintances” in the sense of this copyright exemption (§ 52a para. 1).¹⁴⁹⁵ At the hearing on § 52a copyright draft law (ver. 16/8/2002) the representatives of the movie industry expressed their fear that this copyright exemption would support the piracy and illegal distribution of their contents on the schoolyard.¹⁴⁹⁶ This is justified with the assumed possibility that movies could be stored in the intra-net of the school and could be downloaded. Only the argument would be put forward that these films would be used in the classes, the content providers stated.

The Copyright draft law (ver. 16/8/2002) plans that only parts of copyright protected IP may be taken without financial compensation. This would also endanger the primary market, as the content providers explain. It would be the responsibility of the editorships in the publishing houses to select the text passages, examples and cases of exercise in such a way that they correspond to the special educational requirements.¹⁴⁹⁷

In opinion of the VdS even a financial remuneration instead of free uses of IP according to the copyright exemption would not solve the problem of the economic disadvantages for the publishing industries.¹⁴⁹⁸ The individual remuneration of these uses is organizationally not possible because of the multiplicity of computers in schools, educational facilities and universities. The collective and flat-rate remuneration would only pay minimum amounts. They could not adjust the financial losses. The cancellation of § 52a would be easily possible, because this copyright exemption is not compellingly prescribed by the EU Copyright Directive.

The movie industry declined the § 52a. If it is not canceled, they demanded a separate treatment of movies to protect their business models and the subsequent utilization of their works (cinema, DVD, pay-TV, free TV etc.). Their appeal was successful.¹⁴⁹⁹

The supporters of this paragraph come from the libraries, universities, scientist, research groups etc. According to their argumentation, the education and research would inadequately be obstructed without the paragraph. Without it they would have to acquire single licenses with the right owner for each edu-

¹⁴⁹⁴ See: VdS (2002); *Verlage und Wissenschaftler für ein faires Urheberrecht* (2003); BITKOM, BDI, VDZ, BDZV, VdS (2002).

¹⁴⁹⁵ See: BVV (2002).

¹⁴⁹⁶ See: Kreutzer (2002).

¹⁴⁹⁷ See: VdS (2002).

¹⁴⁹⁸ See: VdS (2002a).

¹⁴⁹⁹ See: *Böhm* within this book on page 520; Krempf (2003).

ational use.¹⁵⁰⁰ With the Hochschulrektorenkonferenz (HRK), a late supporter of this exemption arrived on the political stage. They criticised the Federal Ministry of Justice for not inviting them to the hearing held on October 15th 2002.¹⁵⁰¹ In the aftermath, the HRK published statements on § 52a.

An absence of the exemption according to § 52a would possess similar negative consequences for libraries. If bought electronic publications could not be made accessible in the library nets, the libraries would be unable to accomplish their duties to inform the public. Consequently a large part of the population would not be able to participate in the information society.¹⁵⁰² Furthermore, if the uses according to the copyright exemptions depend on the agreement of the right holders, the libraries would be confronted with numerous treaty negotiations, disproportionate prices and with an extensive administration. They claim that they would be unable to overcome this administrative problem.¹⁵⁰³

Also some legal scientists supported this copyright exception. For example Professor Hoeren and the Institut for legal questions of the free and open source software (ifrOSS) published supporting statements.

IfrOSS welcomes the regulations of § 52a copyright draft law (ver. 6/11/2002).¹⁵⁰⁴ The right holders would profit from the exemption if an appropriate remuneration is defined. If the exemption does not exist and if the single use of the IP is not controllable, then illegal uses would increase, assumes IfrOSS. Then the right holders would not be compensated at all. If the use according to the exemption is permitted and compensation is realized by a flat rate remuneration, then the right holders would benefit financially. This argument could also be stated concerning the private copy exemption. IfrOSS expects no significant abuse of this exemption. Therefore it would come to no excessive uses to the disadvantage of the right holders.¹⁵⁰⁵ They justify this with the restriction of the privilege on the required purpose and the defined user circle.

In the political conflicts even the commercial attaché of the US embassy in Germany, David Nelson, intervened. He sent letters to members of parliament and to the Federal Ministry of Justice. He warmly recommended the cancellation of § 52a.¹⁵⁰⁶ The American publishers of educational and scientific works would fear financial losses of one of their most important markets. He also stated that § 52a would not comply with international copyright law.

Representatives of the Federal Ministry for Justice explained that the exemption had to correspond to the requirements of the practicability. Un-enforceable prohibitions make no sense.¹⁵⁰⁷ The prohibition demanded by the right holders is not effective because of the uncontrollability.

¹⁵⁰⁰ See: Kreutzer (2002).

¹⁵⁰¹ See: HRK, Landfried (2002).

¹⁵⁰² See: BDB, DBV, DGI (2002). See also: EDB (1998).

¹⁵⁰³ See: Beger (2002).

¹⁵⁰⁴ See: ifrOSS, Jäger, Kreutzer (2002): 5.

¹⁵⁰⁵ See: id. 7f.

¹⁵⁰⁶ See: Krempl (2003).

¹⁵⁰⁷ See: Kreutzer (2002).

During the legislative procedure, the § 52a was changed in several ways.¹⁵⁰⁸ Finally, the provision was temporarily limited until 31. December 2006. In the meantime, both the limitation and the provision could be changed by the parliament if the monitoring in the code of practice or abuse of the provision demanded it.¹⁵⁰⁹ Because of this limitation and legal arrangement the parties involved would attempt to induce the political parties and the government to change the provision. Political conflicts will be on the agenda.

In the parliamentary ballot in the Bundestag the faction of the political party FDP declined to accept the copyright act mainly because of the § 52a. They criticised that it goes to the costs of the authors.¹⁵⁰⁹

The CDU/CSU opposition stated that they only approved the Copyright Act in the Bundestag because of the temporary limitation of the provision § 52a. Previously they had demanded its cancellation.¹⁵¹⁰ In their decline of § 52a they follow the argument of the publisher of educational and scientific works that the primary market of these publishers would collapse.

Finally, the copyright exemption of § 52a was not abandoned but watered down.¹⁵¹¹

III.3 Enforcement of Copyright Exemptions in DRM-Systems

The restriction of the legal protection against the circumvention of technical measures in favour of copyright exemptions was one of the most contentious aspects in the negotiations at the WIPO and the European Union.¹⁵¹² At the European Union a compromise between these two alternatives became generally accepted: In principle the technical measures for the protection of digital goods have priority in contrast to the enforcement of copyright exemptions. It is forbidden to circumvent them. No “right to hack” is defined in the copyright law, even if the political party Bündnis 90 / Die Grünen, which is part of the government, demanded it. The junior partner in the German government could not accomplish their aims on this issue during parliamentary debates.¹⁵¹³

However, the right holders are taken into the obligation by the EU copyright directive: Based on voluntary agreements they have to allow copying in accordance to certain copyright exemptions.¹⁵¹⁴

The copyright draft law supports use contracts. The right owner will require the completion of a contract with the user prior to usage. In the contract, the prohibition of the circumvention of technical protection measures and the exact

¹⁵⁰⁸ See: *Böhm* within this book on page 520.

¹⁵⁰⁹ See: Bundestag — Rechtsausschuss (2003).

¹⁵¹⁰ See: Krempl (2003).

¹⁵¹¹ See: *Böhm* within this book on page 520.

¹⁵¹² See: Metzger (2001).

¹⁵¹³ See: Krempl (2003).

¹⁵¹⁴ See: Art. 6 para. 4 EU Copyright Directive. Note: The legal regulations for the guarantee of copyright exemption within technical protection measures were discussed in the article by *Goldmann* within this book on page 502.

use conditions of digital contents are fixed. The EU copyright directive and the German copyright draft law leaves the question relatively open, to what the copyright exemptions for private copying can be circumvented by use contracts. To what extent use contracts can cancel the permission of the private copy is differently answered, whether the copyright exemption will be circumvented by technical protective systems or by use contracts. They may not be circumvented by technical protection measures.¹⁵¹⁵ According to the EU Copyright Directive and the copyright draft law (ver. 6/11/2002¹⁵¹⁶) a technical protection system do not have to permit uses appropriate to the copyright exemptions if the content provider deploy use contracts. Nevertheless, lawyers have difficulties with the question whether the use contracts may actually circumvent all copyright exemptions.¹⁵¹⁷

	Approval of the enforcement of the copyright exemption for private copying in DRM-systems	Refusal of the enforcement of the copyright exemption for private copying in DRM-systems
Authors	DJV ¹⁵¹⁸	
Content providers		IFPI ¹⁵¹⁹
Users	VZBV ¹⁵²⁰ BDB, DGI ¹⁵²¹ DBV ¹⁵²²	
Others		Forum der Rechteinhaber ¹⁵²³ GVU ¹⁵²⁴

Tab. 4. Enforcement of the Copyright Exemptions for Privat Copying in DRM-Systems

The VPRT welcomes that the enforcement of the private copy (§ 53 para. 1) is not in the catalog of privileged copyright exemptions which are to be guaranteed even in technical protection measures. The association also approves that the draft law does not contain a self-help right to enable the user to enforce the copyright exemptions (right to hack). Otherwise DRM systems could be circumvented on a broad basis, the VPRT stated.¹⁵²⁵

¹⁵¹⁵ See: § 95 b. para. 1. copyright draft law (ver. 6/11/2002).

¹⁵¹⁶ See: § 95 b. para. 3. copyright draft law (ver. 6/11/2002).

¹⁵¹⁷ See: Günnewig, Hauser, Himmelein (2002): 18–19.

¹⁵¹⁸ DJV (2002a): 5.

¹⁵¹⁹ Braun (2002): 160; IFPI (2002e); IFPI (2002d); IFPI (2002); IFPI (2002c): 2.

¹⁵²⁰ See: VZBV (2002a); VZBV (2002).

¹⁵²¹ See: Beger (2002).

¹⁵²² See: DBV (1999); DBV (1999a)

¹⁵²³ See: Forum der Rechteinhaber (2002): 7-8; id. (2002b).

¹⁵²⁴ See: GVU, Scharringhausen (2002). GVU, Tielke (2002).

¹⁵²⁵ See: VPRT (2002a).

The IFPI, the Forum der Rechteinhaber, and an ad-hoc-alliance of content providers and the BITKOM¹⁵²⁶ criticize the obligation for the supply of technologies for the circumvention of technical protection measures. Thus copyright exemptions were raised to juridical enforceable requirements without practical necessity. By that the requirements of the European Union copyright Directive were clearly exceeded.¹⁵²⁷ The Forum der Rechteinhaber calls the right an over safety device of the interests of individual user groups. Thus the legislator would correspond too much to the interests of individual user groups, criticized the Forum der Rechteinhaber.¹⁵²⁸

IFPI, SPIO/film 20, VPRT and the mentioned ad-hoc-alliance demand that the enabling of uses according to the copyright exemptions should not be obligating, but only an unsolicited action.¹⁵²⁹

The Forum der Rechteinhaber and the VPRT suggest independently from each other an alternative system to enable uses according to copyright exemptions. In principle, the volunteer actions should have priority. Therefore, experts and parties involved have to take part actively.¹⁵³⁰ Thus the actions for enabling copyright exemptions, which are necessary according to § 95b para. 1 copyright draft law, have to be formalized in negotiations between associations of right holders and associations of the beneficiaries of the copyright exemptions. There is the danger that the parties involved achieve no agreement due to conflicting interests. In this case, a solution has to be created by a conciliation procedure. The advantage of this solution is its flexibility.¹⁵³¹

However the permission to use IP according to copyright exemptions, even if copy protection and use use contracts are present, is endorsed by libraries and the consumer protection. Without such a regulation the copyright exemptions would be worthless in their opinion, because they could be easily prevented.¹⁵³²

IV Individual vs. Flat Rate / Collective Remuneration Systems

In the context of the amendment of the German copyright law according to the EU copyright directive one most substantial conflict regarding the application DRM systems exists. It is a conflict on the question to what extent it leads to a change of the remuneration system. It is discussed if the existing flat-rate and collective remuneration systems enabled by collecting societies could be substituted by a individual system put into practice by DRM-systems.

¹⁵²⁶ Members of this ad-hoc alliance are BITKOM, BDI, VDZ, BDZV, VdS.

¹⁵²⁷ See: IFPI (2002c); IFPI (2002); Forum der Rechteinhaber (2002b).

¹⁵²⁸ See: Forum der Rechteinhaber (2002b). Note: a similar argumentation could be found at VPRT. See: VPRT (2002b): 4.

¹⁵²⁹ See: SPIO, Film 20 (2002c); BITKOM, BDI, VDZ, BDZV, VdS (2002); VPRT (2002a); VPRT (2002b).

¹⁵³⁰ See: Forum der Rechteinhaber (2002b); VPRT (2002a); VPRT (2002b).

¹⁵³¹ See: VPRT (2002b).

¹⁵³² See: BDB, DBV, DGI (2002).

The permission for being allowed to make copies for the private uses the legislator links with an obligation: The right owner should get a financial compensation for this uses. For this in Germany a collective remuneration system was established, which is realized by collecting societies. The core of the system is a collective and flat-rate levy on devices and blank media, which must be paid by the producer or importer. This type of remuneration is regarded as an important source of income in particular for the creators.¹⁵³³

Usage cannot be determined in this system, which photocopying devices were used, and to what extent contents are duplicated, or to what extent special tape decks were used for copying. Therefore on the sales of a tape recorder and of storage media an flat-rate levy is raised. Thus it is not differentiated, whether a photocopying device only multiplies self-written texts, or IP of other right holders are extensively copied. Thus the charge is flat rate levied.

The remuneration of the right holders is also flat-rated. They are not paid according to the actual use according to copyright exemptions of their works. On the basis of a complex and complicated system the collecting societies determine, how high the portion of the work of the total duplication are, and the remuneration is paid accordingly.

DRM systems are discussed to replace this flat-rate system within the digital area by the technical implementing of an individualized remuneration system. The collection of the levies and the remuneration of the right holders are to take place depending upon the concrete and individual utilization of the copyright exemptions. The individual licensing of uses according to the copyright exemption is discussed in particular within the area of the private copy.

The considered statements refer usually to the discussion of the advantages and disadvantages of the collective remuneration system and the DRM systems for these uses. The core conflict is the evaluation of the question, which of the two remuneration systems should be used. The question occurs who has to pay the remuneration. In the last consequence the consumer pays the remuneration instead of the right holder. Depending upon the remuneration system another participant is responsible to drive it: In the case of the adoption and retention of the flat-rate levy the ICT industry would be responsible to collect it. This industry could either add the levy on the selling price of devices or blank storage media or it could reduce its profits. In the case of the individual remuneration the contents providers could re-compensate it to the other right holders. They would retain and remunerate the levy individually for each use according to the copyright exemptions.

The central conflict parties in the debates about the remuneration system are BITKOM and the collecting societies.

¹⁵³³ See: ifrOSS, Jäger, Kreutzer (2002).

BDI¹⁵³⁴, DIHK¹⁵³⁵ and BITKOM¹⁵³⁶ reject the copyright levy on ICT devices. They demand the individual licensing system which should be enabled by DRM-systems.

The IFPI, the Forum der Rechteinhaber and the VPRT endorse individual remuneration systems where it is technical and economically realizable.¹⁵³⁷

On the other hand the Kulturrat,¹⁵³⁸ GEMA,¹⁵³⁹ ver.di¹⁵⁴⁰ and VG Wort¹⁵⁴¹ advocate the levy on ICT. Some time after this interest expression, the GEMA joined the Forum der Rechteinhaber. The GEMA represents thereby also its political aims.

The proponents and opponents of the flat-rate remuneration system pursue various argumentations:

Decline of the remuneration by a levy on ICT	Approval of the remuneration by a levy on ICT
Criticism of the remuneration by a levy on ICT	Debilitation of the critics of of the opponents of the levy-system
Advantages of the individual system enabled by DRM	Disadvantages of the individual system enabled by DRM
earlier: ICT devices like CD-burner are not appointed for copying according to the copyright exemptions	
	Advantages of the levy system
	Advantages of the collecting societies

Tab. 5. Chains of Argumentation

Two groups exist who demand which remuneration system should be used for the digital area. The first group is the ICT industries and the commercial users: BITKOM, BDI and DIHK. The members of the BITKOM would have to pay the flat rate levy. The DIHK and BDI represent users of ICT technologies which are produced by the members of BITKOM. They would have to pay the levy indirectly because of higher selling prices. The second group cannot be described

¹⁵³⁴ See: BDI (2000a); BDI (2002): 110; Holeweg (2002): 157; BDI (2002a); BDI (2002b); BDI (2000a); BDI (2002).

¹⁵³⁵ See: DIHK (2002): 116f.

¹⁵³⁶ See: BITKOM (2001i); id. (2002e); id. (2002b): 113, 115; id. (2000a); id. (2001); id. (2002c); id. (2002f); id. (2001i); id. (2002c); id. (2002e); id. (2001h); Harms (2002); id. (2002b): 112; Druck Gegen Abgaben (2001); id. (2001a); id. (2001b); id. (2001c); id. (2001d); id. (2002); id. (2002a).

¹⁵³⁷ See: IFPI (2002e); Forum der Rechteinhaber (2002); VPRT (2002a).

¹⁵³⁸ See: Kulturrat (2000).

¹⁵³⁹ See: GEMA (2002): 56

¹⁵⁴⁰ See: verdi (27.01.1997); verdi (2002a): 66.

¹⁵⁴¹ See: VG Wort (2002): 92.

precisely. It consists of the Collecting Societies (GEMA and VG Wort), the authors (ver.di) and the Kulturrat¹⁵⁴².

The other parties involved — like the content providers, the consumers and the corporate users — discuss the concrete remuneration system only at the edge. Instead, they discuss the permission of the copyright exemptions.

The levy is discussed for ICT which are used for copying like scanners and CD-burner. A substantial argument of the BITKOM against flat-rate levies on ICT is that the users of CD burners pay with its purchase for the option to copy according to the copyright exemptions even if they do not use this option.¹⁵⁴³

The Landgericht Stuttgart (regional court) dealt with a law-suit referring to the levy on CD burners. This was in 2001 and stated that CD burners are for copying destined devices and that a levy has to be paid to them to compensate uses according to the copyright exemptions.¹⁵⁴⁴

Starting from this judgment the BITKOM no longer asked the question in the center of its argumentation whether certain ICT devices are intended for copying and thus the levy on them is required. Instead the BITKOM and its members strongly promoted the application of DRM systems. They referred to the operational readiness of the systems. Besides, they emphasized the advantages of the individual and the disadvantages of the flat rate remuneration system.

Flat-rate copyright levies for ICT and the system change from a flat rate to an individual remuneration system were also subject of a mediation between the BITKOM and the collecting societies GEMA, Wort and Bild-Kunst. The BITKOM accomplished that the subject of the procedure was the question, whether the system change could be made in foreseeable time by the application of copy-protection- and DRM-systems.¹⁵⁴⁵ Appropriate regulations should be taken up to the amendment of the copyright law according to the demand of the BITKOM. The collecting societies successfully objected to this in the mediation. They did not want to be specified on an obligatory exit from the system of the ICT-levy. Therefore the formulations to the future system change were not sufficient for the BITKOM.¹⁵⁴⁶ Therefore it left the mediation because a system change was not fixed.¹⁵⁴⁷ Representatives of the Federal Ministry of Justice demanded renewed discussions — but unsuccessfully.¹⁵⁴⁸

The opponents of the flat rate levy enumerate a number of negative consequences of this system and the levy on ICT devices. The proponents of the ICT-levy try to weaken the arguments.

¹⁵⁴² The Kulturrat organizes collecting societies and authors.

¹⁵⁴³ See: N.N. (2000).

¹⁵⁴⁴ See: Urteil des Landgerichts Stuttgart (2001): 616–618; Flechsig (2001): 656f; Kröber (2000): 545.

¹⁵⁴⁵ See: BMJ (2002).

¹⁵⁴⁶ See: id.

¹⁵⁴⁷ See: Wilkens, Zota (2002).

¹⁵⁴⁸ See: Krempl (2002c); BMJ (2002).

	Stand	Agree	Disagree
1	Distortion of competition to the disadvantage of the German ICT industries in the EU internet market	BDI ¹⁵⁴⁹ BITKOM ¹⁵⁵⁰ D21 ¹⁵⁵¹ DIHK ¹⁵⁵² Druck gegen Abgaben ¹⁵⁵³	GEMA ¹⁵⁵⁴ IG Medien ¹⁵⁵⁵ VG Wort ¹⁵⁵⁶
2	Consumers would buy abroad	BDI ¹⁵⁵⁷ BITKOM ¹⁵⁵⁸	GEMA ¹⁵⁵⁹ VG Wort ¹⁵⁶⁰
3	Movement of companies abroad, loss of jobs	BITKOM ¹⁵⁶¹ Druck gegen Abgaben ¹⁵⁶²	IG Medien ¹⁵⁶³ VG Wort ¹⁵⁶⁴
4	Counter productive for the development of the information society	BDI ¹⁵⁶⁵ BITKOM ¹⁵⁶⁶	IFPI ¹⁵⁶⁷ VG Wort ¹⁵⁶⁸
5	Wrong signal to the users ¹⁵⁶⁹	BITKOM ¹⁵⁷⁰ DIHK ¹⁵⁷¹	
6	Inflexible system, little consideration of the actual use of IP ¹⁵⁷²	BITKOM ¹⁵⁷³	

Tab. 6. Consequences of the System of Levies on ICT

¹⁵⁴⁹ See: BDI (2000a).

¹⁵⁵⁰ See: N.N. (2001a); Kreml (2002a); ZVEI (2000); Zecher (2002): 455; BITKOM (2001j): 40; id. (2000a); id. (2002f); id. (2002); id. (2002c); id. (2002e); id. (2002b): 113; id. (2001i); id. (2001j): 40; (Hoeren (2001): 33).

¹⁵⁵¹ See: Persson (2000).

¹⁵⁵² See: DIHK (2002): 117; (See also: DIHK (2002): 117).

¹⁵⁵³ See: Druck gegen Abgaben (2001c); id. (2002).

¹⁵⁵⁴ See: GEMA (2002): 56f.

¹⁵⁵⁵ See: verdi (2002a): 66.

¹⁵⁵⁶ See: VG Bild-Kunst, VG Wort (2000).

¹⁵⁵⁷ See: BDI (2002): 110.

¹⁵⁵⁸ See: BITKOM (2001a); id. (2000a); id. (2002b); id. (2002f); id. (2002e); id. (2002): 113, 116; id. (2001j): 40f; id. (2000a); id. (2001); id. (2002e); Bode (2001); Kuri (2001j); Harms (2002).

¹⁵⁵⁹ See: GEMA (2002): 57.

¹⁵⁶⁰ See: VG Wort (2002): 93.

¹⁵⁶¹ See: BITKOM (2000); id. (2000a); id. (2002c); id. (2002e); id. (2002b): 113; Zecher (2002): 455.

¹⁵⁶² See: BDI (2002): 110.

¹⁵⁶³ See: BITKOM (2000a); BITKOM (2002); Sibold (2001).

¹⁵⁶⁴ See: IFPI (2002a): 36.

¹⁵⁶⁵ See: VG Wort (2002): 92

¹⁵⁶⁶ See: Gerber (2002); Druck Gegen Abgaben (2002).

¹⁵⁶⁷ See: Persson (2000).

¹⁵⁶⁸ See: Thoms (2002): 157.

¹⁵⁶⁹ Note: The users could believe that they are allowed to copy as much as they want, because they have already payed the copyright levy with the purchase of the device.

One of the main arguments of the ICT industry is that in the European internal market the competition was distorted to their disadvantage, if copyright levies should be raised on their products.

The Bundesrat (Upper House of Parliament) took position on this topic. It explained that the height of the levy would charge German ICT companies with high domestic market share more, than foreign competitors. The latter would only have to pay a levy for imported goods to Germany.¹⁵⁷⁴

A further argument is that consumers would buy the ICT–devices abroad,¹⁵⁷⁵ which would mean financial disadvantages for the industry. This is a smaller problem for the IT industry, than for the retail trade. The German ICT industry also sells its products as an exporter without an appropriate copyright levy to the retail trade abroad. It sells the devices to the customers without arising a levy. Thus, the foreign retail trade can sell the ICT–devices lower–priced to the consumers than the German retail trade. Kathrin Bremer, formerly responsible for copyright issues in the BITKOM, explained that the levy could not simply be added to the price of IT devices, reasoning that this is hardly enforceable in view of Asian and European competition.¹⁵⁷⁶

The assumed distortion of the competition and the drift of consumers abroad as a result of the ICT–levy are two of the reasons, why the ICT industry threaten to relocate their companies abroad. Therefore, the state would lose revenues and jobs. Furthermore negative consequences would result for the development of the information society. Besides, the ICT–levy would be a false signal to the consumers. Furthermore, the consumers could falsely believe that as much as desired might be copied, after the copyright levy was already paid for the devices and blank media.

A further point of criticism to the flat rate remuneration system is that the actual use is not determined. Instead the collection and remuneration occurs flat rate. This argument leads already to the advantages of DRM systems, which work against this problem.

The IT industry sees in DRM systems and in the associated individual remuneration system a solution for the problems of flat–rate remuneration systems.

¹⁵⁷⁰ See: BITKOM (2001j): 40.

¹⁵⁷¹ See: DIHK (2002): 117.

¹⁵⁷² Note: It is not considered whether with the devices such material is copied, which is protected by copyright.

¹⁵⁷³ See: BITKOM (2000a); id.(2002a): 3; id. (2002b): 112, 114; id. (2002c); id. (2002f); id. (2001j): 41; Harms (2001).

¹⁵⁷⁴ See: Bundesrat (2002b).

¹⁵⁷⁵ See: Druck Gegen Abgaben (2002).

¹⁵⁷⁶ See: Zecher (2002): 455.

1	User pays only for the actual use according to copyright exemptions	BITKOM ¹⁵⁷⁷
2	Right holders get remuneration according to the actual use according to copyright exemptions	BITKOM ¹⁵⁷⁸
3	The relationship between IP and appropriate remuneration of the author is clarified to the consumer	BITKOM ¹⁵⁷⁹ DIHK ¹⁵⁸⁰
4	Reduction of the administrative costs	BITKOM ¹⁵⁸¹

Tab. 7. Advantages of the Individual Remuneration System Enabled by DRM-Systems

Above all, ICT companies endorse the application of DRM systems and the associated individual remuneration system: DRM is regarded as a technical measure, in order not to have to pay levies on devices or blank media or to pay as small levies as possible.

BITKOM, BDI and DIHK endorse the individual remuneration. As one of the most important arguments for DRM systems the supporters call the possibility of the proof of the actual utilization of copyright exemptions. Besides, the DRM systems have to help to reduce administrative expense of the collecting societies by the use-referred collection and remuneration. Thus, the individual remuneration is fairer, both for the right owner and for the user of the work.¹⁵⁸² For example consumers and companies would not have to pay a levy for uses which are not taken up. This is one of the main points of criticism of BDI and DIHK, whose members would have to pay the levy as users of ICT-devices.

The content providers could only react on the arguments of BITKOM, BDI and DIHK. The advantages enumerated by the supporters of the DRM systems are not brought up for discussion directly by their counterparts promoting a levy-system. Instead additional points of criticism at the application of the DRM systems for enabling an individual remuneration system are brought forward.

In opinion of the BITKOM¹⁵⁸³ and the BDI¹⁵⁸⁴ flat-rate remuneration systems are only acceptable in such areas, where an individual licensing is actually impossible. A similar position is represented by IFPI,¹⁵⁸⁵ Forum der Rechtein-

¹⁵⁷⁷ See: BITKOM (2001); id. (2002); id. (2002c); id. (2002b): 112, 114; N.N. (2001); Harms (2002).

¹⁵⁷⁸ See: BITKOM (2002a): 3; id. (2002d); id. (2002f); id. (2002b): 112; id. (2002); Harms (2002).

¹⁵⁷⁹ See: BITKOM (2001); id. (2002); id. (2002d); Harms (2001);

¹⁵⁸⁰ See: DIHK (2002): 117.

¹⁵⁸¹ See: BITKOM (2001).

¹⁵⁸² See: Druck Gegen Abgaben (2001b); id. (2001d).

¹⁵⁸³ See: BITKOM (2000a); id. (2002b): 112.

¹⁵⁸⁴ See: BDI (2002): 110; Holeweg (2002): 157.

¹⁵⁸⁵ See: IFPI (2002e); Gerber (2001); IFPI (2002a): 36; Braun (2002): 166; IFPI, GEMA (2002).

haber¹⁵⁸⁶ and the collecting societies VG Bild–Kunst¹⁵⁸⁷ and GEMA¹⁵⁸⁸: Content which could not be protected by technical measures would have to be recompensed by a levy. So far only BITKOM, BDI and DIHK explained that already today an individual system could be guaranteed by DRM systems in the digital area.

1	Application of DRM systems for the remuneration can be economically substantially more expensive, as the right perception by collecting societies	DJV ¹⁵⁸⁹ ver.di ¹⁵⁹⁰
2	Actual DRM systems cannot replace the data bases and documentation nets maintained by the collecting societies, without which no licensing and no appropriate distribution of the remuneration is possible	GEMA ¹⁵⁹¹
3	None of the DRM systems would be able to fulfill the cultural and social tasks of the collecting societies	GEMA ¹⁵⁹² ver.di ¹⁵⁹³
4	Probably no other system would be subject to control as strong as the collecting societies	GEMA ¹⁵⁹⁴

Tab. 8. Disadvantages of the Individual Remuneration System Enabled by DRM–Systems

The importance of the system of the collecting societies within the digital area is also discussed in connection to the conflicts of interests regarding the two remuneration systems. Primarily parties involved gave comments on the role of the collecting societies, which want the flat rate remuneration system to be maintained also within the digital area. GEMA,¹⁵⁹⁵ bvKamera,¹⁵⁹⁶ Kulturrat¹⁵⁹⁷, djv¹⁵⁹⁸ and ver.di¹⁵⁹⁹ explained that the system of the collecting societies had worked satisfying and is needed within the digital area.

The supporters of the displacement of the flat rate by individual remuneration systems do not state explicitly that the collecting societies are completely without any duties in the digital area.

¹⁵⁸⁶ See: IFPI (2002d); Forum der Rechteinhaber (2001); id. (2002): 4–6; id. (2002a); Becker (2002).

¹⁵⁸⁷ See: VG Bild–Kunst (2002): 5–6.

¹⁵⁸⁸ GEMA is a member of the Forum der Rechteinhaber.

¹⁵⁸⁹ See: DJV (2002a): 7.

¹⁵⁹⁰ See: verdi (2002b).

¹⁵⁹¹ See: Becker (1999): 55.

¹⁵⁹² See: Becker (1999): 55.

¹⁵⁹³ See: verdi (2002b).

¹⁵⁹⁴ See: Becker (1999): 55f.

¹⁵⁹⁵ See: Becker (2000): 33.

¹⁵⁹⁶ See: bvkamera (2002).

¹⁵⁹⁷ See: Kulturrat (2002a): 17; id. (2002); id. (2002b).

¹⁵⁹⁸ See: DJV (2002a): 7.

¹⁵⁹⁹ See: verdi (27.01.1997).

However, their demand leads to the fact, that a substantial business field of the collecting societies do not apply, the remuneration of exemption uses like the private copy.

In the discussions it is also demanded to reduce the extent and the level of the levy on ICT and blank media the further DRM systems are in use. This leads at the same time to an expansion of the duties of the collecting societies. The collection and above all the distribution of the raised levies are thereby very complicated. This applies at least until the DRM systems are far common in use for individual remuneration.

Becker of the collecting society GEMA explains that in the digital area a fragmentation of the copyrights is present. This makes it more difficult for the right holders to administrate their rights individually and the individual right acquisition for the user of the contents.¹⁶⁰⁰ Becker justifies it with the multiplicity of IP and the innumerable (international) right holders.¹⁶⁰¹

The tasks of the collecting societies exist not only in the right perception for the right holders but also in the right assignment for the work users. These rights to use must be acquired by the user from the owner. This task can be fulfilled in opinion of Becker best by the VGen.¹⁶⁰² DRM system providers promise that this task can also be fulfilled by the right holders if they use DRM systems.

In the discussion it is referred to the cultural and social tasks of the collecting societies. Therefore, they promote for example culturally valuable works or support artists in states of distress. These tasks are legal target regulations.¹⁶⁰³ Kreile and Becker of the GEMA do not interpret them as a target regulation, which rules in the free legal discretion of the collecting societies.¹⁶⁰⁴ Most German collecting societies, as for example the GEMA, the VG Bild-Kunst and the VG Wort fulfill this function according to their statutes.¹⁶⁰⁵

It was already addressed that DRM systems are designed to allow a direct compensation according to the actual exploitation of copyright exemptions. From the taken levies the collecting societies do not only take the administrative expense off — whose reduction the proponents of the application of DRM systems promise. They also finance cultural and social purposes with that money. The taken revenues for uses according to copyright exemptions are to be disbursed one-to-one to the rights holders. In the remuneration system of the collecting societies the appropriate incomes are distributed in accordance with the principle that culturally meaning works are to be promoted. Therefore an one-to-one disbursement of the revenues is not possible.¹⁶⁰⁶ The same applies for social aims.

¹⁶⁰⁰ See: Becker (2002).

¹⁶⁰¹ See: Kreile, Becker (1997): 636f; Leßmann (2001): 18; Meyer (2001): 17.

¹⁶⁰² See: Becker (2002).

¹⁶⁰³ See: §§ 7, 8 UrhWahrnG

¹⁶⁰⁴ Kreile, Becker (1997): 633.

¹⁶⁰⁵ See: Satzung GEMA; Satzung VG Bild-Kunst; Satzung VG Wort. See also: Becker (2002).

¹⁶⁰⁶ See: Gerlach (2002).

It is also possible that the right owners are obligated to pay such levies for cultural and social purposes to the collecting societies even if DRM systems are used. In this case they could fulfill cultural and social purposes. According to the law in force this represents a problem because it concerns only a target regulation.

DJV,¹⁶⁰⁷ *ver.di*,¹⁶⁰⁸ BDI¹⁶⁰⁹ and VPRT¹⁶¹⁰ demand that double remunerations have to be avoided. Therefore they require that the amount of the levy on ICT should adapt to the extent as technical protection measures for the work concerned are used (refer to the actual application of DRM systems).

Contrary to this position the BITKOM demands that the ICT-levy should not apply if effective technical protection measures exist which the author could use for individual licensing of uses according to the copyright exemptions (refer to the availability of DRM systems).¹⁶¹¹ If the condition is that DRM systems must be available it means at the same time that the application of DRM systems is actually obligating. It is not obligating by law, however a financial incentive exists. Only those right owners would be recompensed for uses according the copyright exemptions, which use the DRM systems.

The political party CDU stated, that the individual remuneration system should take priority over the flat rate and collective remuneration system. They consider DRM-Systems as the future of the protection of authors.¹⁶¹²

In February 2003 — just before the adoption of the amendment of the German Copyright Act — the arbitral board of the German Patent and Trade Mark Office¹⁶¹³ published an arbitrage: It contains a proposal for a levy on computers amounting to 12 Euro.¹⁶¹⁴ After this decision the discussion regarding the levy and the change from a flat rate and collective remuneration system to an individual remuneration systems enabled by DRM-Systems has raised again. Some parties involved published statements on the arbitrage. BITKOM and the IT company Hewlett Packard declared that they would not accept the arbitrage.¹⁶¹⁵ Because of a small margin the computer manufacturers would have to pass the levy directly to the consumers. Whereas the collecting societies Wort and Bild-Kunst approved the arbitrage.¹⁶¹⁶ Ferdinand Melichar, general manager of the collecting society Wort, stated that the decision of the arbitral board would be pathbreaking.

The political discussions regarding conflicts of the amendment of the German Copyright Act were concentrated on the remuneration system and the change

¹⁶⁰⁷ See: DJV (2002a): 7, 8.

¹⁶⁰⁸ See: *verdi* (2002a): 66.

¹⁶⁰⁹ See: BDI (2002).

¹⁶¹⁰ See: VPRT (2002b).

¹⁶¹¹ See: BITKOM (2001i).

¹⁶¹² See: Ziegler (2003).

¹⁶¹³ Note: In German: Schiedsstelle des Deutschen Marken- und Patentamts.

¹⁶¹⁴ See: Kuri (2003a).

¹⁶¹⁵ See: Kuri (2003). Wilkens (2003).

¹⁶¹⁶ See: Wilkens (2003).

from a collective and flat-rate system to a DRM enabled individual system. Since the adoption of the EU Copyright Directive the discussions raised. The main conflicting parties were the collecting societies and the BITKOM who represents the German ICT-industries. The right holders themselves, like the DMV and the German IFPI remained in the background at this stage. After the Copyright Draft Law of the German Government of 16th August 2002 the political conflicts regarding the ICT went into the background. The Government introduced a new copyright exemption in favor of education and reasearch (§52a)¹⁶¹⁷ At this stage, it was obvious that the individual system is a perspective for the future which would have to be discussed in the second legislative procedure even if the BITKOM and the political parties FDP and CDU/CSU would have liked to regulate it in the first Copyright Act.

An interim solution or acceptable solution is probable, with which both the flat rate system is maintained, and the individualized system is used. This can be justified with the fact that unprotected IP will be present for long time parallel to DRM protected IP. For example IP which can not later be subjected to the protection, that was present before technical protection systems were widely spread. This applies at least until PC and other output devices no longer play unprotected content.¹⁶¹⁸

IV.1 Evaluation of the Technological Status Quo of DRM-Systems

The parties involved and the political decision makers evaluate the level of the development of the DRM systems very different. However the evaluation of the level of development is in the political conflicts very important. One group in the political conflicts would like to achieve a system change from the flat-rate to the individual remuneration system. In order to provoke the legislator for it, the representatives of this group have to prove the the readiness of the DRM-systems convincingly.

However the question is problematic, when the technical conditions and the security of the DRM system are acceptable for the parties involved. It is in such a manner problematic, since it is also always a political decision.

¹⁶¹⁷ See: *Böhm* within this book on page 520.

¹⁶¹⁸ See: Plura (2002): 186; *Kuhlmann, Gehring* within this book on page 178.

The stated interests of the participant involved can be summarized in two positions:

	Actual DRM systems are technically not developed, unreliable and not operational	DRM systems are available and proven at present
Authors	bvkamera ¹⁶¹⁹ DJV ¹⁶²⁰ ver.di ¹⁶²¹	
Content Providers	Börsenverein ¹⁶²² IFPI ¹⁶²⁴ VDZ ¹⁶²⁵	Musikverleger-Verband: ¹⁶²³
Users		BDI ¹⁶²⁶ BITKOM ¹⁶²⁷ DIHK ¹⁶²⁸ Druck Gegen Abgaben ¹⁶²⁹
Collecting Societies	GEMA ¹⁶³⁰ VG Bild-Kunst ¹⁶³¹ VG Wort ¹⁶³²	
Others	Kulturrat ¹⁶³³ VPRT ¹⁶³⁴	

Tab. 9. Evaluation of the Technological Status Quo of DRM-Systems

This table shows the following: The operational readiness and a sufficient security of the DRM systems are confirmed by those parties, which endorse the use of

¹⁶¹⁹ See: bvkamera (2002).

¹⁶²⁰ See: DJV (2002a): 7.

¹⁶²¹ See: verdi (2002a): 65; verdi (2002b).

¹⁶²² See: Börsenverein (2002a): 16; Prietze (2000).

¹⁶²³ See: Musikverleger-Verband (2002): 40.

¹⁶²⁴ See: BMJ (2000): 38; IFPI (2001); Schaefer (2000).

¹⁶²⁵ See: VDZ (2002): 85.

¹⁶²⁶ See: BDI (2002): 110; BDI (2000a).

¹⁶²⁷ See: BITKOM (2001j): 40. See also: id. (2000a); id. (2001); id. (2002); id. (2002a): 3; id. (2002b); id. (2002d); id. (2002b): 112, 115. id. (2002a): 4; Harms (2001); Bremer (2002): 163.

¹⁶²⁸ See: DIHK (2002): 117.

¹⁶²⁹ See: Druck Gegen Abgaben (2001); id. (2002a).

¹⁶³⁰ See: Becker (2002a): 164; Becker (2002); GEMA, VG Wort, VG Bild-Kunst (2002).

¹⁶³¹ See: VG Bild-Kunst (2002): 5. Note: In a statement the VG Bild-Kunst explain that applicable and functional DRM systems only exist within the music sector for the distribution of music from electronic data bases over the Internet. In addition, they were used here only to a small extent. See similar: Wilkens (2003).

¹⁶³² See: Thoms (2002): 157, 161.

¹⁶³³ See: Kulturrat (2002b).

¹⁶³⁴ See: VPRT (2002): 88.

DRM systems. However the opponents do not judge it as technically matured and uncertainly. The latter argue with the fact that security measures could be broken with special hacker tools within a short time (ver.di¹⁶³⁵).

On the issue of whether DRM systems are properly developed and secure, to date, has been written. The majority of the publications were given a lot by the parties involved. They are often political motivated¹⁶³⁶ and independent assessments of the security of DRM systems are in short supply.

Even the Federal Minister of Justice Zypris does not assume that DRM systems are not fully developed.¹⁶³⁷

IV.2 Privacy in DRM-Systems

DRM systems could endanger the privacy of the users in the Internet. At least the members of the International Working Group on Data Protection in Telecommunications fear this.¹⁶³⁸

DRM can compensate the individual use of IP according to copyright exemptions and charge the user individually. To accomplish the financial transactions personal data of the user are required. With this data personal profiles regarding the use of IP can be collected. Supporters of these profiles emphasize that better offers can be provided to the user, which reflect past usage. However critics explain that anonymous purchases such as Playboy via a digital kiosk will no longer be possible, if DRM systems are in place.

Supportors of this use of the personal data draw a comparison with the mail order: Mail order companies know, who their customers are and which goods they order. For example the Internet bookseller Amazon knows the past purchase behavior of its customers. They use this knowledge in order to offer them new publications and other books they maybe interested in.

The consequences of the application of DRM systems for the privacy of the consumers were hardly brought up for discussion in the political conflicts. Only the commissioners for data protection and privacy as well as ver.di took up this topic in their statements.

Ver.di only dealt with this topic as a preferal issue. The trade union explained that DRM systems would produce data streams and controllability, which were not compatible with the principles of data security law.¹⁶³⁹ Ver.di uses the data security and privacy argument in order to refer to disadvantages of the application of DRM systems.

¹⁶³⁵ See: verdi (2002a): 65.

¹⁶³⁶ See: Pfitzmann, Federrath, Kuhn (2002); Krempl (2002d); Sieber (2002); DMMV, VPRT (2002); DMMV, VPRT (2002a); Felsenberg (2002); BITKOM, TÜViT (2001).

¹⁶³⁷ See: Bundestag (2002).

¹⁶³⁸ See: Krempl (2001). Note: The legal challenges of DRM systems for the privacy was already discussed in article by *Bygrave* on page 418.

¹⁶³⁹ See: verdi (2002b).

The commissioner for data protection and privacy of the German federal state Brandenburg demands the guarantee of protection of the users from espionage of personal data about the individual use of content and from the production of user profiles.¹⁶⁴⁰ This view is also held by the Bundesrat.¹⁶⁴¹

The commissioner for data protection and privacy of the German federal state “Berlin” explained that the German commissioners favoured such solutions for the remuneration of the authors, which get along without personal data.¹⁶⁴² Therefore levies on ICT were supported.

At first, it is a surprise why the critics of the DRM systems do not use the argument of an imperiled privacy more strongly. Little attention is given to the privacy problem because the topic is not a copyright problem, but a data security–legal problem. Therefore, it is not considered in connection with the amendment of the German copyright law.

IV.3 Legal Protection against the Circumvention of Technical Measures

The prohibition of the circumvention of technical protection measures via the so called legal anti–circumvention provisions are demanded by members of all parties involved: Content provider (IFPI,¹⁶⁴³ VUD¹⁶⁴⁴, DMMV¹⁶⁴⁵), commercial users (BITKOM,¹⁶⁴⁶ DIHK¹⁶⁴⁷), Collecting Societies (GEMA¹⁶⁴⁸) and of the other groups Kulturrat,¹⁶⁴⁹ Forum der Rechteinhaber¹⁶⁵⁰ and VPRT¹⁶⁵¹).

DMMV, VPRT and the Forum der Rechteinhaber are three of the few parties involved, who took care of this topic comprehensively and endorse clarifications in the law. For example they demand the removal of one element of the § 95a para. 1 of the copyright draft law (ver. 6/11/2002) which they characterize as subjective.¹⁶⁵² In this paragraph the prohibition of the circumvention of technical measures is bound to the condition that the contravener intended the circumvention actively. They criticize that the intention of assertion of the user was not present cannot be disproved by the content provider in many cases.

¹⁶⁴⁰ See: Dix (2002).

¹⁶⁴¹ See: Bundesrat (2002b). Note: Upper House of Parliament.

¹⁶⁴² See: Krempl (2001).

¹⁶⁴³ See: IFPI (2002d); IFPI (2002e); IFPI, GEMA (2002). See also former statements of the association and its representatives: Schaefer (2000); Zombik (1998); Morrell (2001); IFPI (2001); IFPI (2001a); IFPI (2001a); IFPI (2001c); IFPI (2002a): 36.

¹⁶⁴⁴ See: Achilles, Schäfer, VUD (2001).

¹⁶⁴⁵ See: DMMV (2002a).

¹⁶⁴⁶ See: BITKOM (2002); BMJ (2000): 43

¹⁶⁴⁷ See: DIHK (2002a).

¹⁶⁴⁸ See: GEMA (2002): 56.

¹⁶⁴⁹ See: Kulturrat (1998); id. (2002b).

¹⁶⁵⁰ See: Forum der Rechteinhaber (2001); id. (2002a); id. (2002): 4; id. (2002b).

¹⁶⁵¹ See: VPRT (2002): 88.

¹⁶⁵² See: DMMV (2002a); VPRT (2002b); Forum der Rechteinhaber (2002b).

The DMMV demands to extend the circle of the technologies protected against circumvention by payment systems.¹⁶⁵³ Besides, the DMMV demands to define the forbidden circumvention purpose more precisely on the basis of a definitive catalog of criteria. There would be the danger that such devices could be improved with additional add-ons. Thus the illegal intention of the devices could be masked.¹⁶⁵⁴ Without a catalog of criteria the intended purpose of a circumvention device is hardly possible. In opinion of the DMMV the criteria have to be formulated with broad participation of the market participants involved. The SPIO/film 20 criticize that a gap in the law develops, if the spreading of circumvention measures are not prohibited in non-profit cases.¹⁶⁵⁵

The prohibition of the circumvention of technical measures is criticized by the *Chaos Computer Club*. It calls this an endangerment of the scientific research on IT-security technologies.¹⁶⁵⁶ Also the DRM conference 2002 in Berlin dealt with the topic. At the conference the scientists Drew Dean¹⁶⁵⁷ and Niels Ferguson¹⁶⁵⁸ referred to the example of the US-American DMCA to give an impression of negative consequences on the scientific research on IT security systems due to anti-circumvention regulations.¹⁶⁵⁹ Ferguson circumvented according to his statement the HDCP copy protection of Intel. The independent cryptography consultant did not publish some results of his research because of his fear of being accused if he entered the USA. His freedom to travel is more important to him, particularly because he frequently works in the USA.

Drew Dean attributed the loss of his job and legal costs of 17.000 US-dollar were due to the publication of results of his research. These results explain how certain watermarking technologies can be circumvented. The lawsuit against Drew Dean and the director of the researcher team Edward Felten was developed on the basis of the anti-circumvention regulations within the US-American DMCA. This act would obstruct the scientific research and the freedom of expression the Electronic Frontier Foundation explained. A legal team of this civil rights organisation for the digital area defended Felten in this case.¹⁶⁶⁰

In accordance with the reason of the copyright draft law (ver. 6/11/2002) such circumvention acts are not punished, which do exclusively have scientific purposes. The Amsterdamer Professor for law Hugenholtz explained that the EU copyright directive does not have comparable negative consequences for the research as the DMCA. That cryptographic research cannot be a cause for a law suit.¹⁶⁶¹

¹⁶⁵³ See: DMMV (2002a).

¹⁶⁵⁴ See: id.; DMMV, VPRT (2002).

¹⁶⁵⁵ See: SPIO, Film 20 (2002c).

¹⁶⁵⁶ See: Krempl (2002): 19; Hummel (2002).

¹⁶⁵⁷ See: Dean (2002).

¹⁶⁵⁸ See: Ferguson (2002).

¹⁶⁵⁹ See: *Becker, Günnewig* within this book on page 655.

¹⁶⁶⁰ See: N.N. (2001b).

¹⁶⁶¹ See: Hugenholtz (2002). *Becker, Günnewig* within this book on page 655.

The problems regarding the scientific research on technical protection measures are hardly addressed in discussions. Only the Forum der Rechteinhaber (forum of the right holders) explained that the permission of circumvention activities, which do serve exclusively scientific purposes (e.g. cryptography) are not to be complained in principle.¹⁶⁶² They also criticised it could be maintained by authors that the evasion from scientific motives take place, in order to examine the security of the assigned technology.

The forum suggested to take an objective element into the law. Therefore, the products of an circumvention for scientific purposes should be destroyed immediately. On the other hand scientific research needs the possibility of publishing the results. This is necessary in order to be able to occupy statements about the security of the systems. In this way research work of other scientists would be possible, which are based on these results.

V The Conflicts of Interests in the Law Making Process

Statements on the implementation of the EU Copyright Directive were published by the parties involved in several stages:

1. 20th December 1996 —
World Intellectual Property Organization — Treaties (WIPO Copyright Treaty (WCT) and WIPO Performances and Phonograms Treaty (WPPT))
2. 17th June 1998 —
European Commission Green Paper on Copyright and the Challenge of Technology
3. 7th Juli 1998 —
Draft of a German Copyright Law by the Federal Ministry of Justice
4. 5th July 2000 —
Second report on the copyright remuneration published by the Federal Government of Germany
5. 22nd Mai 2001 —
EU Copyright Directive
6. 18th March 2002 —
Draft of a German Copyright Law by the Federal Ministry of Justice
7. 22nd April 2002 —
Hearing of the Federal Ministry of Justice on the implementation of the EU Copyright Directive
8. 16th August 2002 —
Draft of a German Copyright Act by the Federal Ministry of Justice
9. 27th September 2002 —
Statement of the Federal Council of Germany (upper house) on the draft law (version 16/8/2002)
10. 15th October 2002 —
Hearing of the Federal Ministry of Justice on § 52a of the bill of a German Copyright Act (ver. 16/8/2002)

¹⁶⁶² See: Forum der Rechteinhaber (2002b).

11. 6th November 2002 —
Draft of a German Copyright Act (ver. 6/11/2002) by the Federal Ministry of Justice
12. 14th November 2002 —
First reading of the Draft of a German Copyright Law (ver. 6/11/2002) in the German Parliament (Bundestag)
13. 29th January 2003 —
Hearing of the committee on legal affairs of the German Parliament on the German Copyright Act (ver. 6/11/2002)
14. February 2003 —
The arbitratative board of the German Patent and Trade Mark Office¹⁶⁶³ published an arbitrage. It contains a proposal for a levy on computers amounting to 12 Euro.¹⁶⁶⁴
15. 14th March 2003 —
Proposal for a new German Copyright Act by rapporteurs of the coalition parties of the German Parliament (SPD, Bündnis 90/die Grünen¹⁶⁶⁵) — Draft of a German Copyright Act (ver. 14/3/2003)¹⁶⁶⁶.
16. 9th April 2003 —
Committee on legal affairs of the German Parliament (Bundestag) determined the proposal for a new German Copyright Act by rapporteurs of the coalition parties (see 14th March 2003) — Draft of a German Copyright Act (ver. 14/3/2003)
17. 11th April 2003 —
Final Readings (2nd & 3rd) and Adoption of the Draft of a German Copyright Law (ver. 14/3/2003) in the German Parliament (Bundestag)¹⁶⁶⁷
18. 23rd May 2003 —
Statement of the Federal Council of Germany (upper house) on the New German Copyright Act Bundestag decision (version 14/3/2003), call for the conciliation committee of the German parliament (Vermittlungsausschuss)¹⁶⁶⁸
19. 2nd July 2003 —
Decision of the conciliation committee of the German parliament (Vermittlungsausschuss)

¹⁶⁶³ Note: In German: Schiedsstelle des Deutschen Marken- und Patentamts.

¹⁶⁶⁴ See: Kuri (2003a).

¹⁶⁶⁵ German political parties.

¹⁶⁶⁶ Note: After discussions with the political factions of the Bundestag, CDU/CSU and FDP the rapporteurs of the coalition parties SPD and Bündnis90 / Die Grünen published a proposal which was adopted by the Committee on legal affairs of the German Parliament (Bundestag) on 9th April 2003. See: BMJ (2003). BMJ (2003a).

¹⁶⁶⁷ The decision of the New German Copyright Act of the Bundestag was transferred to the Bundesrat (upper house of parliament). The was not adopted by the decision yet.

¹⁶⁶⁸ See: Bundesrat (2002).

20. 11th July 2003 —

Final Adoption of the New German Copyright Act in the Federal Council of Germany (upper house)

At every stage the amount of the parties involved which publish their statements increased. Since the publication of the Copyright draft law the Federal Ministry of Justice (18th. March 2002) the statements of the parties involved have changed only marginally.

The amendment of the German legal framework of copyright occur against the background of various international treaties. It aimed in the ratification of two treaties of the World Intellectual Property Organization (WIPO), which Germany had already signed: WIPO Copyright Treaty from 20th December 1996 (WCT) and WIPO Performances and Phonograms Treaty (WPPT) from the same day. The EU Copyright Directive, adopted on 22nd May 2001, builds up on these treaties. The EU Directive should have been already implemented into German Law by the end of December 2002.¹⁶⁶⁹ For the implementation of the directive into German law the Federal Ministry of Justice published a draft law on 18th March 2002. Even before the election to the German Parliament (Bundestag) in September 2002 the draft was brought into the Bundestag on 6th August 2002. The Copyright draft law was transferred to the Federal Council of Germany (upper house, Bundesrat), who took a stand on it at 27th September 2002. The first reading of the new draft (6th November 2002) of the German government took place in the new elected parliament (Bundestag) on 13th November 2002. In this connection the Bundestag answered the statement of the Bundesrat.

Between the various draft laws of an amendment of the German Copyright Act several hearings of the Federal Ministry of Justice, of the German Parliament and of political parties took place in Berlin. In the meantime which the parties involved published written statements and tried to lobby their interests. The parties involved also organized parliamentarian evenings, published special campaign websites and spread flyers in computer stores¹⁶⁷⁰ or published surveys to corroborate their position. For instance the IT company Hewlett-Packard invited the members of parliament and their staff to a “*DRM breakfast*” on 13th December 2002.¹⁶⁷¹ The objective of the breakfast was to overcome objections against DRM-systems.

However the parties involved did not only have the opportunity to bring forward their interests to the political decision makers. They were also able to attend several private conferences which were organized in Germany on this topic. At these conferences they had the opportunity to state their objectives in public. At these conferences several questions regarding the amendment of the German Copyright Act according to the EU Copyright Directive were discussed.

¹⁶⁶⁹ See: Art. 12. para. 1. EU Copyright Directive.

¹⁶⁷⁰ Note: For example the “Initiative Druck gegen Abgaben” (initiative of printer companies against levies) brought out their position regarding the levy on flyers which were allot in 1000 shops. See: Initiative Druck Gegen Abgaben (2002).

¹⁶⁷¹ See: Krempl (2002f).

Agreements of interests between some involved parties also could be found. In the “Forum der Rechteinhaber” some associations from the print and music industries as well as from the collecting societies organized themselves.¹⁶⁷² The participating parties co-ordinated their objectives and interests as far as possible. They published the results of the agreements in joint written statements. Between the joint statements the members of this forum also published individual statements especially on the reprography and other not yet mentioned parts of the amendment of the German Copyright Act.¹⁶⁷³

The agreements of interests in such a forum do have positive effects on the assertiveness of its members and their political impact. The political decision makers concedes that several parties of the policy field could agree on a certain position even when they had to fight some conflicts of interests. This also assists the legislator since he does not have to deal with the various interests and prospectus of single parties but with the result of agreements of interests between parts of the spectrum of parties.

The group of the IT-industries — consisting of the DIHK, the BDI and the BITKOM — is confronted with a much more difficult situation to assert its own prospectus and interests in the public debates against the profoundly organized interests of the right holders. However, the BITKOM succeeded to form a ad-hoc-alliance together with the BDI, VDZ, BDZV and the VdS. In this alliance the previously published statements of its members are repeated and published under the common name of the alliance. The members had not to concede like other members of the participants of the forum of the right holders had.

Even before the publishing of the EU Copyright Directive several written and spoken statements on the issue “Digital IP” were published. Several national, European and international associations assigned statements to the representatives of the WIPO, the EU in the run up of the WIPO treaties and the EU Copyright Directive. After the publishing of the Greenbook of the European Commission on Copyright and related rights, an intensive consultation process took place in which even several German parties, like the German collecting societies were enlisted.¹⁶⁷⁴ Furthermore, a copyright draft law was published by the German government on 7th July 1998. It builds up on the draft for an EU-Copyright Directive which was discussed at that time.

The same applies for the second report on the copyright remuneration of the Federal Government of Germany of 5th July 2000. In this report the government suggested to levy several ICT-devices.¹⁶⁷⁵ The report also rejected demands of some parties to forbid digital copies generally. The parties involved commented on the report in their written statements.

¹⁶⁷² Note: Members of the forum are: Bertelsmann AG, Börsenverein, Bundesverband der Phonographischen Wirtschaft, Musikverleger-Verband, GEMA, GÜFA, GVL, GWFF, IFPI, VdS, VFF, VG Bild-Kunst, VGF, VG Wort, VUT und ZPÜ.

¹⁶⁷³ See: Forum der Rechteinhaber (2002b).

¹⁶⁷⁴ See: Becker (2000): 30.

¹⁶⁷⁵ See: Goffart, Steinbeis (2000). Vahldiek (2000).

The WIPO treaties and the EU Copyright Directive shorten the possible objectives of the parties involved. Especially the EU Copyright Directive concedes certain policy- and legal options while others are restricted, in favour of the harmonization of the national copyright systems. The directive demands from the parties involved which contravene against the regulation of the copyright EU Copyright Directive not to be assertive. This applies especially for those parts of the directive which have to be implemented into national copyright law. Those parts of the EU Copyright Directive which do have interpretation clarification bring again a renewal of the conflicts of interests. The question about the validity of certain copyright exemptions was already discussed during the decision making process of the EU Copyright Directive and are again set on the political agenda in the connection of the German legislation process.

At the same time as the implementation of the EU directive into German copyright law was discussed, a political mediation was taking place on the question of the remuneration of special ICT-technologies. In the procedure the BITKOM and the German Collecting Societies participated.

The subject of the political mediation was extended by request of the BITKOM whether the existing flat rate remuneration system — in the form of levies on ICT and blank media — can be replaced within the digital area in foreseeable time by a functioning system of the individual remuneration of the right holders. According to the view of the BITKOM in this mediation this should be done by copy protection and DRM systems.¹⁶⁷⁶ Thus one of the substantial conflicts regarding the amendment of copyright law was discussed in these committees. The former Minister of Justice, Herta Däubler-Gmelin, was the mediator. However, BITKOM said, that the formulations of the mediation about the future system change did not go far enough and as a consequence the mediation failed.¹⁶⁷⁷

Different parties, like the VdS and the libraries, reacted to the introduction of a copyright exemption in favor of education and research as regulated in § 52a of the Copyright draft law. This aspect contained so much conflict potential that its own hearing was held on 16th October 2002.

Prior the bill being presented to the Bundestag, the Ministry of Justice was responsible for the implementation of the EU Copyright Directive into German law. The Federal Ministry for Economics and Labor (Bundesministerium für Wirtschaft und Arbeit (BMWA)) and the Federal Ministry for Consumer Protection (Bundesministerium für Verbraucherschutz, Ernährung und Landwirtschaft) were only junior partners during the development of the draft laws for the amendment of the German copyright law. The BMWA and the Federal Ministry for Consumer Protection were consulted within the framework of the rules of internal procedures of the Federal Government.

Once the Copyright draft law was brought to the Bundestag the parliament was responsible for the further decision making process. Accordingly the lobbying efforts of parties involved were no longer directed primarily to the originating

¹⁶⁷⁶ See: BMJ (2002).

¹⁶⁷⁷ See: id.

Federal Ministries. They referred their lobbying efforts to the political parties and the delegates of the crucial committees of the Bundestag instead. In the Bundestag the legal committee was responsible, while in the Upper House of Parliament the economic committee¹⁶⁷⁸ dealt with the amendment of the copyright law. The Upper House of Parliament followed the recommendation of the economic committee.¹⁶⁷⁹

The statement of the Bundesrat (Upper House of German Parliament) reflected the argument of the ICT industry in its direction: It demanded that the individual remuneration system should have priority of the the collective and flat-rate remuneration.¹⁶⁷⁹ A further example is that the remuneration over the levies on ICT-devices and blank media has to be reduced if effective technical protection measures exists for the individual remuneration of the right holders.¹⁶⁷⁹ The Bundesrat also agreed — as in the statement of the BITKOM — to the availability and not to actual application of technical protection measures.

The parliamentary group of the SPD in the Bundestag (Lower House of German Parliament) criticized the statement of the Upper House of Parliament.¹⁶⁸⁰

After the second and the third reading of the copyright draft law in the Bundestag the decision was transferred to the Bundesrat where it was discussed again. The Bundesrat criticised some parts of that decision and called for the arbitration panel of the German Parliament.¹⁶⁸¹ The Bundesrat suggested that private copies of copyrighted works are only allowed if they are made of a legal source.¹⁶⁸² According to the Bundesrat private copies should not be possible of illegal sources like some media files in peer-to-peer networks like KaZaA. Furthermore the Bundesrat demands, that it should be forbidden to make private copies by third persons for a beneficiary of that copyright exemption.

Although the first reading of the bill in the Bundestag on 13 August 2002 showed substantial discussions were still needed, after agreement between parliamentary groups of the Bundestag, only half an hour was allocated.¹⁶⁸³ The Federal Minister of Justice, Zypris, defended the draft in the parliament. She stated — like already in the reasons of the draft law — that in this first step only that is to be regulated, what the EU copyright directive and the WIPO treaties compellingly prescribe. A further legislative procedure is to follow, in which these contentious not conversion-requiring questions are to be brought up for discussion and should be regulated.

¹⁶⁷⁸ See: Bundesrat (2002a).

¹⁶⁷⁹ See: Bundesrat (2002b).

¹⁶⁸⁰ See: Bundestag (2002). Key speech in the German Bundestag of Dirk Manzewski (SPD) in the first reading of the copyright draft law (ver. 6/11/2002).

¹⁶⁸¹ This panel consists of members of both houses of parliament who are discussing compromises regarding legislative procedures.

¹⁶⁸² See: Bundesrat (2002); Bundestag (2003). Furthermore, the Bundesrat criticised some parts of the Bundestag decision which are not important for the subject of this article.

¹⁶⁸³ See: Bundestag (2002).

The division of the reorganisation of the German Copyright Act and its adaption according to the challenges of digital IP was affirmed several times during the legislative procedure — and even affirmed in the adopted version of the German Copyright Act.¹⁶⁸⁴ The amendment of the German Copyright Act is divided into two parts. The first stage is to amend the German Copyright Act according to the provisions of the WIPO Treaties and the EU Copyright Directive. It aims in bringing the amendment to a quick end without too many interminable discussions between the legislator and the parties involved. After the adoption of the first stage the second stage would be filled with all the controversial issues which were disregarded in the first legislative procedure. It would start in autumn 2003.¹⁶⁸⁵

“*Aha, Schmalspur!*” (I see, small-time) — This objection during the first reading of the copyright draft law (ver. 6/11/2002) of the member of parliament Kampeter of the CDU/CSU¹⁶⁸⁶ Bundestag faction refers to a conflict in the conflicts of interests.¹⁶⁸⁷

Several parties wanted to let further contentious issues regulate by this amendment of the copyright law. Examples for further contentious issues are digital press mirrors or above all the quality of the digital private copy. They do not want to postpone these issues up to the second legislative procedure. Beside the CDU and also the FDP¹⁶⁸⁸ criticized the copyright draft law in this connection.¹⁶⁸⁹

Even if certain regulation contents are shifted to the second legislative procedure, a certain legal situation is fixed at the same time and their discussion is deferred to the law making process following on. This applies in particular regarding the question whether the enforcement of the copyright exemptions is to apply also to the digital private copy if technical protection systems are used. The digital private copy could have been defined in the catalog of special copyright exemption which have to be guaranteed by the content companies that use DRM- and copy-protection systems. But the law maker has not defined it as such a exemption. In the second legislative procedure where possible negative effects would result from their permission could have been examined.¹⁶⁹⁰ But the new German Copyright Act first correspondents in favour of the interests of the right holders and not of the users.

In opinion of the government parliamentary factions of SPD and Bündnis90/Die Grünen, the copyright draft law (ver. 6/11/2002) accomplishes a reconciliation of

¹⁶⁸⁴ See: Bundestag — Rechtsausschuss (2003).

¹⁶⁸⁵ See: Krempl (2003); Bundestag — Rechtsausschuss (2003).

¹⁶⁸⁶ Political Parties.

¹⁶⁸⁷ See: Bundestag (2002).

¹⁶⁸⁸ Both are political parties.

¹⁶⁸⁹ See: Bundestag (2002). Key speeches in the German Bundestag of Rainer Funke Member of Parliament (FDP) and Dr. Günter Krings Member of Parliament (CDU/CSU) at the first reading of the copyright draft law (ver. 6/11/2002).

¹⁶⁹⁰ See: ifrOSS, Jäger, Kreutzer (2002): 19.

interests between all parties concerned by copyright.¹⁶⁹¹ The CDU/CSU and the FDP parliamentary groups do not see exactly this reconciliation reached, which is what the Upper House of Parliament also determined in its statement.¹⁶⁹² The two parliamentary groups and the Upper House of Parliament demand therefore that the government revisit and discuss with a better participation of all relevant parties involved.

The CDU/CSU opposition in the Bundestag criticized that since the WIPO treaties of 1996 little progress had been made and time wasted by the the European Union and also the Federal Government. The participation of the parties involved should have taken place since the adoption of the treaties and the directive as continuous process. These discussions would have been led also parallel to the European Union consultation on national level even without knowing the concrete arrangements of the directive. Some of the contentious questions were already well-known since the WIPO contracts. “*After such long time we and above all the authors, artist and publisher could have expected that a comprehensive and balanced bill is submitted.*”¹⁶⁹³ Dr. Günter Krings of the CDU/CSU stated.

Nevertheless, the CDU/CSU parliamentarians places themself against the fact that the law is now being fast tracked and driven by the parliamentary consulting procedure.¹⁶⁹⁴ Their parliamentary group demanded further hearings of experts. After the first reading of the copyright draft law (ver. 6/11/2002) in the Bundestag on 14th November 2002, it was transferred for consultation to the responsible legal committee, as well as to the committee for economics and labour, the committee for consumer protection, nutrition and agriculture and to the committee for culture and media.

The discussions in the legal committee of the Bundestag were as controversial as the discussions at the different stages before. The preliminarily acme of the controversies was reached at the hearing of the committee on 29th January 2003. Eighteen experts were named by the various factions of the Bundestag. They represented the structure of the parties involved. The statements of the experts and representatives of the parties involved did not bring up new issues. They only repeated the interests they had expressed in several written and verbal statements before.

¹⁶⁹¹ See: Bundestag (2002). Note: Key Speeches of Grietje Bettin, Bündnis 90/Die Grünen and Dirk Manzewski (SPD) at the first reading in the Bundestag.

¹⁶⁹² See: Bundestag (2002). Key speeches in the German Bundestag of Rainer Funke Member of Parliament (FDP) and Dr. Günter Krings Member of Parliament (CDU/CSU) at the first reading of the copyright draft law (ver. 6/11/2002).

¹⁶⁹³ German Original: “*Nach so langer Zeit hätten wir und vor allem die Autoren, Künstler und Verleger erwarten können, dass uns ein umfassender und ausgewogener Gesetzentwurf vorgelegt wird.*” Bundestag (2002); Talk of Dr. Günter Krings (CDU/CSU).

¹⁶⁹⁴ See: Bundestag (2002); Key speech of Dr. Günter Krings (CDU/CSU) in the German Bundestag. In German he said: “[...] *im Schweinsgalopp durch das parlamentarische Beratungsverfahren getrieben wird.*”

In the copyright draft law of the government (16/8/2002) a new copyright exemption in favour of education and research was introduced. It became one of the most controversial issues of the Copyright amendment. The Federal Ministry of Justice held a hearing on 15th October 2002 regarding the copyright exemption in favour of education and research §52a. This hearing and statements in the aftermath showed that this exemption is one of the most controversial issues of the first legislative procedure to amend the German Copyright Act.

The hearing of the legal committee on 29th January 2003 and the aftermath showed conspicuous that the conflicts regarding the remuneration system and the change from a collective and flat rate system to a by DRM enabled individual system went into the background. It was obvious that the individual system is a perspective for the future which would have to be discussed in the second legislative procedure even if the BITKOM and the political parties FDP and CDU/CSU would have liked to regulate it in the first Copyright Act. The Copyright exemption in favour of education and research §52a became the most controversial issue of the discussions.

After the hearing of the legal committee the amendment of the Copyright Act was discussed between the political parties to compromise. Under the leadership of the governing political parties SPD and Bündnis90/Die Grünen, which had the majority in the Bundestag a compromise was developed. The governing parties considered in parts the interests the political opponents represented in the discussion. The CDU/CSU opposition faction in the German Bundestag asserted that they accept the compromise proposal “*with a heavy heart*”¹⁶⁹⁵. The proposal was adopted in the legal committee and afterwards in the Bundestag with the votes of the coalition parties SPD and Bündnis90/Die Grünen and the opposition of CDU and CSU as well as FDP voted against it.¹⁶⁹⁶ The FDP stated that they could not bear the provisions regarding the copyright exemption of §52a.

VI Conclusion

An ideal DRM system makes it possible that on the one hand protection of the interests of the right holders by impeding illegal use of IP as extensively as possible and legal use forms and new business models. On the other hand such ideal system should secure at the same time the other side of the interest balance, i.e. the optimal accessibility to IP by the users according to the copyright exemptions.

Legal certainty allows one of the conditions for the content providers to distribute their IP in the Internet and to take on the competition with the illegal nets, in which its goods are free of charge available. Thomas Kleesch explained regarding the juridical insecurity before the adoption of the amendment of the

¹⁶⁹⁵ See: Bundestag — Rechtsausschuss (2003).

¹⁶⁹⁶ See: id.

Copyright Act in Germany that content providers would shrink back from the DRM protected on-line distribution due to possible complaints by end users.¹⁶⁹⁷

One of the major problems is that DRM systems — even in connection with the instruments of the legal and contract-legal protection from circumvention of these technical measures — would still “leak”. From the DRM protected legal distribution platforms and from the copy-protected CDs so far not only appropriate protection measures could be broken by experienced computer users, but also by normal users through easily operated tools. Then available unprotected contents are once again brought into illegal distribution platforms.

The mentioned “*Darknet*” — the net in which copyright protected contents are illegally exchanged — is not considerably affected by DRM systems.¹⁶⁹⁸ Not only the authors of the Darknet article from Microsoft do assume some signs, that the Darknet will further exist also if DRM systems are far spread. The Darknet will continue to offer at a small cost, a high-quality service concerning the illegal distribution of intellectual property to a large group of users. Legal offers will have to compete with illegal offers.

It is not only important to protect the legal offers by law but also to stifle the illegal distribution platforms. The latter cannot only take place contrary to the first by legal regulations and appropriate prosecution sanctions and technical measures. This applies in particular due to the problem of the prosecution in digital nets. Therefore, an important role comes to the business models of the content providers: They must try to create better legal offers for IP, than the illegal networks. The legal reactions are however just as important and necessary as the business models. Here is a load-carrying reconciliation between the interests important. “*In short, if you are competing with the darknet, you must compete on the darknet’s own terms: that is convenience and low cost rather than additional security.*”¹⁶⁹⁹

BITKOM undertakes more political PR measures than other parties in the context of the decision making process public perceptible. (Scientific) Reports are given to press conferences in order to prove the operational and technological readiness of DRM systems. They also try to prove it at computer fairs. The GEMA and the other collecting societies do not try to weaken the surveys of the BITKOM by conducting their own surveys. The BITKOM is driven particularly by the interest that its members do not have to pay or pay as small as possible a levy on IT devices. In order to reach this goal, the BITKOM first tried to let judicially clarify that IT devices are not intended for manufacturing copies and are as all-purpose device therefore not subject for remuneration charges. After this did not receive any consideration in court, the association of IT companies BITKOM attitude focused on DRM systems. According to the conception of the BITKOM they try to make an individual remuneration system possible, which

¹⁶⁹⁷ See: Günnewig, Hauser, Himmelein (2002). Note: Kleesch is responsible for the DRM activities at IBM Germany.

¹⁶⁹⁸ See: *Biddle, England, Peinado, Willman* within this book on page 344.

¹⁶⁹⁹ See: id.

replaces the previous flat-rate and collective system realized by collecting societies — and with it the levies on devices. The BITKOM is therefore the most important supporter of DRM systems.

The content providers also endorse the application of DRM systems, however with another motivation: Only on second position stands their concern in the technical security of the systems and to enable uses according to the copyright exemptions. Primarily they aim, assisted by DRM systems, to improve their business models for the primary market and to earn money in the Internet. To enable uses according to the exemptions is considered rather as an obstacle for the business models and as a potential gateway for so called pirates. But at least the rejecting attitude of the IFPI according to the exemption for private copying speaks for this argument. The contents providers like IFPI und SPIO/Film 20 demand above all a legal framework, which allows a more effective procedure against law breaking and illegal offers possible.¹⁷⁰⁰

At the begining of the discussions between the various parties and the legislator regarding the amendmend of the German copyright act, the main controversial issue was the question if the collective and flat rate remuneration system realized by a levy on ICT and blank media trough collecting societies should be replaced by an individual remuneration system enabled by DRM-systems. The main conflicting parties were the collecting societies on the one side and the ICT-industries with their association BITKOM on the other side. During the political process the controversial issues changed. The primary issue took a backseat in the discussions and the paragraph 52a of the copyright draft became more and more the subject of controversial discussions among the parties involved. Two groups emerged. The libraries and similar parties are on the side of the discussions which approved the §52a and the BITKOM, BDI, VDZ, BDZV, VdS, Börsenverein and SPIO/Film20 are on the other which rejected it. Nevertheless the libraries assert their demand for this exception. A short time before the final debate (2nd and 3th reading) in the Bundestag, the discussions regarding the remuneration system re-surfaced. This happend after the arbitrage board of the German Patent and Trade Mark Office published an arbitrage, which contained a proposal for a levy on computers amounting to 12 Euro.¹⁷⁰¹

Beside those already discussed there are many conflicts remaining, some of which are outlined below:

- In DRM systems all goods could get a similar protection standard as copyright protected works, even if they are not protected by copyright.
- There is the danger that works do not become public domain 70 years¹⁷⁰² after the death of the author, if they are protected with DRM-systems. This would have to be integrated explicitly into the use conditions assured technically by DRM systems. Within the USA the protection time period when a work is protected by copyrighted works was extended several times. It would

¹⁷⁰⁰ See: Spio, Film 20 (2002c).

¹⁷⁰¹ See: Kuri (2003a).

¹⁷⁰² See: § 64. para. 1 German Copyright Act.

be problematic to enable a supplementary enlargement of this period of time because the usage conditions would have to be updated in a technical way. As there is no (technical) connection between the right holder and the file or the application which displays or plays it, this would be impossible.

- Under certain circumstances DRM systems cannot offer any transparency to the consumer over the use restrictions. For example a content provider could ensure that a music piece deactivates itself after five years. This can be done, without knowledge of the consumer at time of the purchase, or it in extensive license regulations contracts.¹⁷⁰³
- DRM systems also bring doubts concerning the archiving of information.¹⁷⁰⁴ Medium changes¹⁷⁰⁵ with only information–technically stored works must be made possible. Otherwise it would be possible, that certain contents could not be used any longer due to restrictions of the right owner.¹⁷⁰⁶
- According the German Constitution applies: Property obligates. If it is not made available in extent to the society, this can lead to disadvantages for individual subpopulations. These disadvantages could support the feared segmenting of the information society (“*Digital Divide*”) in “*information-rich*” and “*information-poor*”.¹⁷⁰⁷

This enumerating shows that on the one hand with the DRM system design a multiplicity of non–technical aspects is to be considered. On the other hand it shows that additional conflicts will result from the application of DRM–systems, that are not in the discussions between the parties involved and the political decision maker. If it would come to the system change to individual collection and remuneration of copyright exemptions — which is promoted by BITKOM — further adjustments are necessary. Examples are the cultural and social purposes of the collecting societies. They are financed by the levies in accordance to the copyright exemptions. The legislator must decide whether these purposes have to be guaranteed also in an individual remuneration system. In this case the legislator would have to modify the target regulation of the German copyrights act to an obligation regulation. A special legal and organizational infrastructure would also be needed.

The legislator explained in the reasons of the German copyright draft law that a second legislative procedure will follow directly. On this procedure some parties involved put their hopes in, who see their interests represented in the law insufficiently. With the first act still no reliable legal framework is present, which considers, the interests of parties involved sufficiently. Too many politically contentious questions are excluded, as for example the private copy. Only the second

¹⁷⁰³ See: Screamer (2001).

¹⁷⁰⁴ See: Committee on Intellectual Property Rights and the Emerging Information Infrastructure (2000): 9.

¹⁷⁰⁵ Medium changes for example from the gramophone record to the tape or the CD.

¹⁷⁰⁶ See: DBV (1999a); DBV (2001).

¹⁷⁰⁷ See: Committee on Intellectual Property Rights and the Emerging Information Infrastructure (2000): 2. Warschauer (2002).

legislative procedure has the potential to address the conflicts of interests. This by no means reduces the future lobbying of the parties involved.

The parties involved will have to spend further financial and personnel resources, in order to succeed in the second legislative procedure. Until the second legal procedure is completed, legal certainty can not be reached.

Before the first ministerial draft bill on the amendment of the German Copyright Law was published, first the author treaty law¹⁷⁰⁸ was amended. This first legislative procedure was also shaped by substantial political conflicts of interests. Obviously the Federal Government did not want to lead a two-front war.

*“The stakes involved in all this are high, both economically and in social terms. Decisions we make now will determine who will benefit from the technology and who will have access to what information on what terms — foundational elements of our future society.”*¹⁷⁰⁹

The political decision makers have to discuss the challenges in their entire complexity: Technology, law, economics and social aims and conflicts interlink. Additionally philosophical and ethical considerations on handling knowledge and intellectual goods in the digital age are necessary.

Only after discussion of the possible strategies regarding the handling of intellectual goods the DRM technology comes again into the game: *“DRM technology must be unimpeachably neutral, that is, it may not in any way give an advantage to any hidden interests [...] it is essential that the DRM technology not give a hidden advantage to the rights management technology provider; Neither a right holder, nor a consumer, nor the DRM technology provider should be able to alter or tamper with any agreed-upon commercial arrangements or impede the expression of any party’s rights or interests.”*¹⁷¹⁰

In the considerations to handling intellectual goods within the digital area, it is important not to forget the consumers. They can accept or reject certain DRM systems and business models of the right owners. As long as the technical protection is not perfect and illegal uses are easily and unobservable possible, this group still has the largest power.¹⁷¹¹

VII Acknowledgement

I am grateful to Tobias Dolch, John Garner, Julie Liu and Alexander Rohra for their valuable help in writing this article.

¹⁷⁰⁸ Urhebervertragsrecht.

¹⁷⁰⁹ See: Committee on Intellectual Property Rights and the Emerging Information Infrastructure (2000): 3. Similar: Hoeren (2002b).

¹⁷¹⁰ See: Garnett (2001).

¹⁷¹¹ Note: The policy-scientific analysis of possible political solutions and strategies follows this overview-like representation of the interests of parties involved and the causes of political conflicts. It is the subject of a doctoral thesis of the author in the political science. For this the interests of the parties involved must be considered, in order to fit in the solution in the politics field policy and participant constellation.

4.4 Copyright Dilemma: Access Right as a Postmodern Symbol of Copyright Deconstruction?

Thomas Hoeren¹⁷¹²

I Access Right — Dogmatically

The first question is whether there exists an access right in copyright law. The issue has been raised by Jane Ginsburg arguing that copyright “is not only a ‘copy’ right, but an access right.”¹⁷¹³ The access right relates to new regulations in Europe, USA and other places based on the WCT and the WPPT.

I.1 WCT and WPPT

The story starts with the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonogram Treaty (WPPT). According to Art. 11 WCT and Art. 18 WPPT, “*contracting parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used [...] in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.*”

WCT and WPPT do not refer to “access” or “access control”. They mention tools which “restrict acts”. In addition, they make reference to acts “permitted by law”. WCT and WPPT provide for a protection of technological measures under the condition that the measures themselves do not interfere with basic provisions of copyright law, in particular the exemptions in favor of users.

The term “access” itself is only used in WCT and WPPT in the provision on the right of communication to the public (Art. 6 WCT and Art 10 WPPT) which includes the “*making available to the public [...] works in such a way that members of the public may access these works from a place and at a time individually chosen by them*”. As an *argumentum e contrario*, it can be concluded that not every “access” amounts to an act which can be controlled by the rights holder. The “access” has to be one where members of the public use the protected products from a place and at a time individually chosen by them. The access is not subject to copyright where it is not an act of “*members of the public, for instance in the case of access via internal and small networks*”.

As a consequence, WCT and WPPT do not contain an access right insofar as the rights holder cannot solely authorize or restrict access; the access of a work depends on the rights holder’s permission *or* statutory authorization.¹⁷¹⁴

¹⁷¹² University of Münster.

¹⁷¹³ See: Ginsburg (1999/2000).

¹⁷¹⁴ See: Ginsburg (2000): p. 4 in note 7: “*Neither the WCT nor the Berne Convention clearly articulate a right to control access*”.

I.2 Europe

In Europe, the discussions have been quite different from that approach. The story began with the Software Production Directive (one of the worst pieces of EU legislation), was changed by means of the Conditional Access Directive and found its foul end in the InfoSoc Directive.

Software Protection Directive

According to Art. 7 (1) of the EU Software Protection Directive, Member States shall provide remedies “against” any act of putting into circulation, or the possession for commercial purposes of, which is to facilitate the unauthorized removal or circumvention of any technical device which may have been applied to protect a computer program.¹⁷¹⁵

The EU institutions regarded this issue as a case of secondary infringement; they even used this legal term in the title of the provision during the drafting period.¹⁷¹⁶ The regulation is strongly linked to unfair competition as both acts mentioned have a commercial impact. No reference is made to “access”. It remains unclear what the protected device is protecting. Therefore, the relationship between Art. 7 and the exemptions embodied in Art. 5 and 6 are unclear.¹⁷¹⁷

Conditional Access Directive

The Council Directive on the Legal Protection of Services based on, or consisting of, Conditional Access,¹⁷¹⁸ has to be taken into consideration.¹⁷¹⁹ It protects conditional access systems, i.e. “*any technical measure and/or arrangement whereby access to the protected service in an intelligible form is made conditional upon prior authorization*” (Art 2 (b)).

The Directive obliges the Member States to prohibit the manufacture, import, sale or possession for commercial purposes of illicit devices (Art. 4 (a)). In Recital 21, it is expressly foreseen that this Directive is “*without prejudice to the application of any national provisions which may prohibit the private possession of illicit devices*”. Consequently, the Directive can only be applied in a business-to-business environment.¹⁷²⁰ In that way, the text relates to a concept which is akin to unfair competition. In addition, the whole directive is not related to copyright law (Recital 21).¹⁷²¹

¹⁷¹⁵ For the implementation, see Art. 66 (5) Greek Copyright Law, art 32a Dutch Copyright Act.

¹⁷¹⁶ See the documentation of draft made by Thomas Vinje (Vinje (1993)).

¹⁷¹⁷ The discussion in Germany and Austria has been resumed by Blocher (2001): Software Art 7, Note 15 with further references.

¹⁷¹⁸ See: Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998, OJ L 320, 28/11/1998, p. 054

¹⁷¹⁹ The European Convention on the Legal Protection of Services based on, or consisting of, Conditional Access, STE 178 of 24 January 2001.

¹⁷²⁰ See: Heide (2000): 993 et seq.; Dusollier (2000): 25 et seq.

InfoSoc Directive

In addition, Art. 6 of the InfoSoc Directive has to be considered.¹⁷²² In conformity with the WCT, the Directive requires the Member States to provide adequate legal protection against the circumvention of any effective technological measures (Art. 6 (1)). Different from WCT, the protection shall include the protection against circumvention tools (Art. 6 (2)). This regulation has nothing to do with copyright law; it is an additional, accompanying measure based on unfair competition. Therefore, the protection against tools only extends to commercial actions, not against private acts.

It should as well be noted that the InfoSoc Directive does not speak of “access”. Unlike Sec. 1201 (a) of the US Copyright Act, it restricts unauthorized “acts” (see Art. 6 (3) (1)). The term “access control” is only used as an example to determine the effectiveness of a technological measure (see Art. 6 (3) (2)). The wording of Art. 6 (3) is clear as it relates to “*prevent or restrict acts [...] which are not authorized by the rights holder*”. The term “acts” itself relates to the traditional exploitation rights. It is for instance used in Art. 5 (1): “temporary acts of reproduction . . .”. or in Art. 5 (2) (c): “specific acts of reproduction”. Therefore, the Directive does not recognize in several Member States (Art. 2-4).

II Access Right — Nationally

II.1 National Regulations

An access right does not exist on a national level either. The USA has provisions that restrict the act of obtaining unauthorized access by circumvention (Sec. 1201 (a) (1)) and the manufacture or making available tools for unauthorized access (Sec. 1201 (a) (2)). These regulations have caused some US courts to speak of a “right to control access” granted to copyright owners.¹⁷²³ These wordings seem however not to have been made to describe a new access right. Apparently, the courts only used the term “right to control access” as an equivalent to the anticircumvention rules of the US Copyright Act (and behind that WCT).

The traditional copyright system does not know an access right apart from the existing rights of reproduction, distribution, public performance or communication to the public. The existing ALAI reports demonstrate at least in Europe, an access right does not exist. The states adapt their traditional system of exploitation rights in order to determine the borderline for the possible use of copyright works.

¹⁷²¹ See § 297 A, 298 of the British CDPA 1988 which proves that the UK misleadingly implemented the Conditional Access Directive by changing the Copyright Act.

¹⁷²² See: Directive 2001/19/EG of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society, OJ L 167 of 22.06.2001, p. 10.

¹⁷²³ See: *Los Angeles Times v. Free Republic*, (54 U.S.P.Q. 2d 8BNA.) 1452, 2000 U.S. Dist. LEXIS 5669 at 67 et seq. (C.D. Cal. 2000); *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 346, 2000 US Dist Lexis 11949 (SDNY August 17, 2000). [Editors’ Note: This case was affirmed sub nom. *Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir 2001).]

II.2 The Term “Access Right”

In addition, I am in doubt whether the term “access right” is useful. Access means traditionally the “way (in) to a place”.¹⁷²⁴ It is thus linked to a certain place, a limited and closed space which has an entrance, a way in. Leaving these territorial roots aside means to use “access” as a metaphor. In fact, there is a legal discussion on “access rights”. But in this context “access rights” relate to the free access of the public to information¹⁷²⁵ and is linked with the freedom of information question.¹⁷²⁶ It is therefore misleading to use that term in sense which is clearly the opposite of freedom of information: an exclusive right to restrict public access.

In addition, “access right” is a term used in relationship to a lot of different access control tools. In her article mentioned above, Jane Ginsburg mentions for instance “pay-per-view/listen systems” or “anti-copying systems”. She additionally mentions “limit[ing] listening or viewing by number of plays, by number of computers on which the work may be played, by duration of access, and so on”. In fact, the concept of access rights has to be distinguished from reprints and permissions, encrypted content solutions, content distribution mechanisms, and copyright enforcement devices.¹⁷²⁷

II.3 Traces of Access Rights

There have been several attempts to combine the concept of access rights with traditional topics.

First Publication

One way of interpreting it was to make a reference to the right of authors to first publication.¹⁷²⁸ However, the right of first publication is a right of first, public access to copyrightable works. The difference with the access right is obvious. The right to first publication only includes.

- first access
- of the public
- to copyrightable works.

This approach does very much to contradict the structure of the “access right”. This right apparently includes.

- any access (even to published works)
- of anybody, even he is a close relative or friend of the creator
- to any work even if it is not copyrightable.

¹⁷²⁴ See the advances Learner’s Dictionary of Curent English, 2 nd ed. 1948, p. 6

¹⁷²⁵ See the title of the work of Marsh (1987).

¹⁷²⁶ For instance Pinto (1984); Mehra (1986).

¹⁷²⁷ See the General Report of Sirinelli (2001): 5 et seq. Further details in Lasica (2001).

¹⁷²⁸ This combination of concepts has been mentioned in the French and the Canadian ALAI report.

Access and Copyright

Moreover, there are clear indications that access rights have nothing to do with copyright protection.

It is the near-future. I am jogging along a tropical beach (which I would never do as I hate jogging). I have my palm-sized book reader player-satellite cell phone that permits instant access through digital networks to an infinite variety of literary works of the 13th century and musical works from the 18th century performed in auditions at the beginning of the 20th century and recorded in 1940.

In spite of the fact that these recordings are in the public domain, I am automatically charged for listening to them or the charge is debited from my account. Although I can read or listen to these works without permission, I have to pay for the access to these works via digital devices. Therefore, the US House of Representatives is right in stating: “*These [...] provisions have little, if anything, to do with copyright law.*”¹⁷²⁹.

Roman Law of Possession

Access rights are in my view deeply rooted in Roman law concepts of possession. If I possess a thing, I can restrict others from using it. If I possess land, I can even build fences to avoid trespassing and control access. Circumvention restriction restrictions in electronic form now allow us to build up electronic fences. However, these fences are not erected in the sense that I possess all these electronic goods used by millions of customers. No, these fences are a symbol for a virtualization of possession, leaving aside the personal relationship between a possessor and “his” land or “his” object.

As a consequence, there is a parallel between possession and access restriction. However, since the ancient times, all civilized countries believe that possession is not a right as such. Possession does not give a right in the object itself, as even a thief can have possession. Possession is only protected insofar as it is formally unlawful and a violation of the personal rights of the possessor to take an object away from the person which possessed it before.¹⁷³⁰ The same applies to “access”. The mere fact that somebody integrated a control mechanism into a digital product doesn’t give him a positive right to control the access to the product. But it might be considered formally unjust that somebody else circumvents or abolishes this access control tool. Therefore, there doesn’t exist a right to control access to copyrighted works. Access control is a mere fact; the big players already control the access to digitized products. The question is whether we want to prevent circumvention devices which are undermining these tools.

But the reference to possession demonstrates further weaknesses of the access right model. If we go back to Roman law of possession, two elements are nec-

¹⁷²⁹ Committee of Commerce of the House of Representatives (July, 22nd 1998): p 24. Similar consideration might be found in Goldstein (1997): 151.

¹⁷³⁰ See: Sohm (1928): 431 et seq.

essary for justifying a legal protection of possessors: “corpus” (detention) and “animus domini”. When industry uses access control systems they do certainly have animus domini; they wish to be the technically dominating Leviathan of the information world. But they don’t have “corpus” in the Roman law sense as all the copies integrating access control systems are in the possession of the users. However, even the Roman law foresaw that in certain cases somebody can be the person who has “corpus” granting him a limited use right (such as a hire or rental agreement). But then we have a major problem for access rights. If industry is really hiring or renting their products to users with an expiration time, they can of course use access control systems for the purpose of stopping the users from using the goods after the expiration date. However, in these cases the companies are subject to severe civil law rules on liability which they don’t like. These companies want to combine the elements of rental (for justifying their expiration dates and the non-applicability of the exhaustion doctrine) with the concept of sale (to determine warranties and contractual liability) by using the nebulous term “licensing” (which doesn’t exist in civil law). But this opt-in and opt-out system doesn’t work. If somebody is going to a record shop and buys a CD, he is a party to a sales agreement. But if he buys the copy, he is entitled to use his property without limitations. Technical control mechanisms can therefore not be justified. But if he gets it with a clear indication that there is an expiration period, he is renting it and he can rely upon the high level of liability in rental contracts (at least in Europe).

Unfair Competition and Trade Secrets

If the law of possession cannot justify access rights, the question remains whether unfair competition law is a reasonable justification. This implies that private use or the actions of researchers (like the case of Dr. Felten¹⁷³¹) are not part of the access control regulations; these activities should be free. There are several courts who referred to common law based trade secret rules as the basis for anticircumvention decisions. For instance, in the DeCSS case a California court decided that CSS is protected as a trade secret under common law.¹⁷³² Similar decisions might be found for instance in Germany where courts referred to unfair competition law to forbid the use of anti-dongle systems in software business.

The trade secret approach is in my view the most convincing perspective. The use of a specific technology integrated in works is strongly linked with the idea that the technology itself should be protected against persons who try to de-

¹⁷³¹ In June 2001 the Electronic Frontier Foundation (EFF) and others filed suit on behalf of Princeton University professor Edward Felten and a team of researchers who cracked the code for the secure Digital Music Initiative (SDMI) watermark, asking for a declaratory judgment that the team has a First Amendment right to share its findings with the world at large. See for details: <http://www.thestandard.com/article/0,1902,27281,00.html> and <http://cryptome.org/sdmi-attack.htm>.

¹⁷³² *DVD Copy Control Ass’n Inc. v. McLaughlin*, 2000 WL 48512, p. 1 (Cal. Sup., Jan. 21, 2000). Available at: http://www.eff.org/pub/Intellectual_property/DVDCCA.case/20000120pi-o-order.html

termine the specific features of the technology and make a business out of their knowledge. However, the trade secret approach leads to further questions I cannot solve in this panel (which is only discussing the mere question whether an access right exists). For instance, it has to be discussed why third parties have to respect trade secrets independent of contractual obligations. Furthermore, a lot of states grant trade secret protection as a kind of property right; but they have to limit this right in consequence of the problem of innocent infringement.¹⁷³³ Furthermore, due to broad extension of the anti-circumvention rules, new limitations have to be created to protect the interests of the public. The case is similar to the new regulations on sports rights where the public interest in important football games is as well protected against the broadcasting of football exclusively by pay-TV-companies.¹⁷³⁴ This question leads to general principles of media law determined partly by the EU Directive on Television without Frontiers.¹⁷³⁵

Let us stop here. No further discussion is needed as the necessary minimum can at least be said: There is no such thing as an access right in copyright law.

III Access Right — Politically

But the question remains whether we want an access right to exist. This is a political issue which is open for discussion.

The big players in the entertainment industry seem to have noticed these problems. They try to solve them by introducing technological measures. That step allows them to integrate their own view of copyright in the programming codes (the famous “code as code” problem of Lawrence Lessig).¹⁷³⁶

The big players have considered the borderlines of copyright law internally for years.¹⁷³⁷ There seems to be a tendency among the “Majors” to focus on technological solutions for that purpose. The technological strategy has some major advantages: The answer to the machine is now in the machine. Lawyers, statutes, courts are no longer needed; technicians are replacing lawyers and programming codes are taking the role of codifications. Technology can be used worldwide — without the limitations of nationally based laws. It is cheap and directly effective. Even if sagas like SDMI suggest that “big players” are in fact having considerable difficulty in preventing hacking,¹⁷³⁸ technological tools still remain effective as to the majority of users and are being adapted regularly to the highest state of the art.

¹⁷³³ See the summary of Dessemontet (1974) : 277 et seq.

¹⁷³⁴ Thanks to Prof. Dr. Jon Bing (Oslo) which led me to this idea after along discussion in the JFK airport after the ALAI conference was finished.

¹⁷³⁵ OJ L 202 of 30 July 1997, 60. Cf. n. Helberger, Study on the use of conditional access systems for reasons other than the protection of remuneration, to examine the legal and economic implications within the Internal Market and the need of introducing specific legal protection, Report presented to the European Commission, April 2000.

¹⁷³⁶ See: Lessig (1999): 3 et seq.

¹⁷³⁷ See: Samuelson (1993): 49.

There are some doubts as to the desirability of these techniques from the perspectives of users *and* creators. Users have to fear that their freedom to use works is undermined as anti-copying devices do not per se take account of statutory exemptions. Strategies which are already in use (like regional encoding techniques) show the power of these tolls which restrict technically what can be done legally (for instance according to the exhaustion doctrine).

The authors have to fear that the producers only use the effects of these tolls for their own sake.¹⁷³⁹ Authors normally don't have the knowledge and money to invest in anti-copying devices. In addition, they are not protected against the contractual buy-out of their rights by the big players. If Microsoft, Sony or other big companies want to get the digital rights, they get them — without any additional payment, any equitable remuneration, with a simple signature on a long standard contract formula.¹⁷⁴⁰ This can be criticized by people who are supporting creative persons (as myself who has worked for years to support the legal interests of documentary film artists). But it is a fact. We only have to be honest nevertheless about which party we are representing and supporting. Please don't lie. In the present situation, access right is a mere discussion for the benefit of the "Majors".

IV Access Right — Deconstructively

But even if there is no such thing as an "access right," isn't there a need to discuss a fundamental change in the copyright structure? Perhaps the whole discussion on "access rights" is only a symbol, a feverous warning, an inherent feeling that copyright law is becoming ill.¹⁷⁴¹ I don't want to stress all the indications that US and European colleagues have described, focusing on the inadequacies of copyright in the digital age.¹⁷⁴² Let only hint at a few symptoms.

The traditional concept of exploitation rights is based upon the copyright industry and their needs at the end of 19th century/beginning 20th century. At the beginning, exploitation via tangible goods (books, music records, paintings) was regarded as being dominant; therefore, the focus in copyright legislation was on reproduction and (in several states) "distribution". It took some time until exploitation in an intangible form was regarded as a major problem. When television and broadcasting came up, the legislators simply added some references to these techniques in their copyright acts.¹⁷⁴³ This led to the incorporation of public performance rights in France and the USA.¹⁷⁴⁴ After cinemas, radio and TV became widespread, the copyright acts incorporated sections on these new

¹⁷³⁸ This remark relates to the case of *RIAA v. Diamond Multimedia Systems*, 180 F. 3d 1072 (9th Cir. 1999), *GRUR Int.* 1999, 974.

¹⁷³⁹ This problem has been neglected in Ginsburg (2000): 9

¹⁷⁴⁰ See: Field (2000): 145 ff.

¹⁷⁴¹ For a radical criticism of copyright law cf. Barlow (2000). Similarly among others Masson (1996): 1049.

¹⁷⁴² See also: Dreier (1993): 15 ff; Ginsburg (1995): 101 ff; *ibid.* (1996): 189 ff.

¹⁷⁴³ See: Ginsburg (2000): 6.

techniques. However, these new rights were only linked to dissemination techniques that allowed for a simultaneous transfer of information to an unlimited number of users. With the internet, it became necessary to provide for a new right of “making available to the public”. Towards the end, WCT and WPPT solved an important issue in promoting such a right.

However, even after the WIPO discussions, the existing system of exploitation rights does not fit the needs of the information society. Take for instance the reproduction right. There is a worldwide discussion about how we can adapt this old right to digital uses. Some people argues that the reproduction right has internal limits where ephemeral copies (such as RAM, proxy storage) are concerned. Representatives of the digital industry (i.e., Microsoft) supported the concept that reproduction is the mega-right in the electronic world, including any temporal reproduction. The WIPO did not find any solution for that problem during the discussions in the WCT/WPPT.¹⁷⁴⁵ The European Commission tried to solve that issue after a harsh debate, by asking if there was any “independent economic value” of transient copies (Art. 5 (1) of the InfoSoc Directive). However, this regulation doesn’t help at all as it will be nearly impossible to determine which digital copy has an independent economic value. In addition, Art. 8 (3) of the InfoSoc Directive supports the claim of rights holders that access providers should be liable for any proxy storage of works in the light of possible injunctions. In my view, it is a pity that future discussions on copyright and digital use depend on the question whether and when a copy has an independent economic value.

Similar considerations have to be taken as to the “making available to the public right” introduced by the WIPO Copyright Treaty. Even this new and broad right will not solve the problem that the traditional concept of exploitation does not suit the needs of the information society. Even in the light of the WCT, there remains the huge problem of deciding what is “public” (i.e. using intranets). Where are the borderlines between public and non-public use? Are for instance intranets, i.e. small intra-corporation networks, directed to members of the public or not? If we don’t solve these difficult issues, the extent of the new making available right remains unclear.

Therefore, I agree with Jane Ginsburg where she describes the different concepts of exploitation rights: “After all, there should be nothing sacred about the eighteenth- or nineteenth-century classifications of rights under copyright, in a technological world that would have been utterly inconceivable to eighteenth-century minds”.¹⁷⁴⁶

An important attempt to solve the issue of new economic rights has been mostly unnoticed although it is clearly embodied in the EU Database Directive, Jens Gaster (European Commission/DG XV) “invented” not only the highly disputed

¹⁷⁴⁴ See the law of January 15, 1791 in France and the US Act of August 18, 1856, ch. 169, 11 Stat. 138.

¹⁷⁴⁵ See for the different opinions, Ficsor (1997): 197; Samuelson (1997): 369, 390 et seq.

¹⁷⁴⁶ See: Ginsburg (2000): 8.

“sui generis right”.¹⁷⁴⁷ He additionally set aside the traditional cluster of exploitation rights by using new terms. Art. 7 of the Database Directive provides that the maker of a database can “prevent extraction and/or reutilization” of the contents of a database. These new terms relate not only to business-to-business situations. As Recital 42 expressly states, it relates also “to any user who, through his acts, causes significant detriment, evaluated qualitatively or quantitatively, to the investment”.

However, several Member States refused to integrate these new rights in their legislation.¹⁷⁴⁸ Especially in Germany, the traditional wording (reproduction, distribution etc.) was used after a long and controversial debate. This change in the terms is a clear violation of the implementation duties of each EU Member State. In addition, this gap demonstrates that many people didn’t notice that the radical new approach in the Directive.

V Access Right — Historically

European copyright concepts are the historical starting point for a discussion on access rights. At the beginning, there was the main principle of freedom of information. Until the Renaissance, everybody could use each book for whatever purpose. Granting monopolistic rights for books was an issue of the 16th century. It is common knowledge that the roots of copyright are linked with the privileges for printers and book traders in Italy, later in the UK and Germany privileges were granted by sovereigns on a national basis. The granting of privileges to printers was linked with the view that these privileges are bound to and have to be used for the “utilitas publica”.¹⁷⁴⁹ A “privilegium onerosum,” to the disadvantage of society, has to be cancelled.¹⁷⁵⁰ Privileges should thus only be granted “in seltenen Fällen” (in rare cases).¹⁷⁵¹

The idea that authors have to be protected as such is a product of the French theory of Enlightenment (“Aufklärung”), the British concept of “literary property” based on John Locke¹⁷⁵² and the German philosophy¹⁷⁵³ of idealism.¹⁷⁵⁴ The three European traditions merged into the idea that the “genius,” the creative author, should be given “geistiges Eigentum,” “propriété intellectuelle,” a protection of its own apart from the protection for printers.¹⁷⁵⁵ However, even until the 19th century there was a pan-European discussion whether the owner of a book copy should be free to reprint it due to his status as the owner.¹⁷⁵⁶

¹⁷⁴⁷ See: Gaster, VPP-Mitteilungen 1996, 112.

¹⁷⁴⁸ See: Raue, Bensinger. MMR 1998. 510.

¹⁷⁴⁹ See: Frohne (1993): 11 ff.

¹⁷⁵⁰ See: Carpzov (1649): 413-416.

¹⁷⁵¹ See: Lamprecht (1784): 322.

¹⁷⁵² See: Kohler (1907): 47 f.

¹⁷⁵³ See: Fichte (1971): 223 ff.

¹⁷⁵⁴ See: Bappert (1957): 75 ff; Vogel (1973): 303 ff; Vogel (1978): 1 ff.

¹⁷⁵⁵ See: Ginsburg (1990): 991 relating to the 19th century roots for determining moral rights in Europe.

Nevertheless, the question arises whether the idealistic model of creativity is still a valid vision for post-modern society. Of course, there are still many individual authors among us, particularly in the literary, pictorial and even musical realms. But these areas have lost their impact compared to the growing phenomenon of “team-creativity”. Movies were the first category of copyrightable works based on inseparable influences of a big team of creator (such as the scriptwriter, the director, the cameraman etc.). The movie world consequently shocked the copyright world so that it took more than fifty years until film works got full protection in international copyright conventions. But the issue of “team-creativity” become even bigger and more threatening with digital technologies. Software, marketing campaigns, applied arts — these works are mostly created by big teams sometimes involving hundreds of developers. This change has to be taken into consideration when discussing the need for a political change in the copyright system.

VI Access Right — Philosophically

VI.1 Copyright Law as One Part of Information Law

Copyright law is thus to be considered as being itself a part of a broader area of law, the information law. Information law is a term which is being discussed more and more worldwide. It is a new model which tries to stress the common lines between the various industries of film, software, telecommunications, media and entertainment. The term “information” is broad and difficult to define.¹⁷⁵⁷ However, recent studies, especially of Jean Nioclas Druey, have demonstrated that it might be possible to explain the content of the term “information” as the bases of a concept of information law in distinguishing between the act of increasing knowledge, the content and the status of having some knowledge.¹⁷⁵⁸ If we use this broad definition, copyright law has to be regarded in a different way than the traditional perspective. Copyright protects information, indeed, it is even the Magna Carta of the information law. However, it has to be considered as only one of various other elements of information law. Media law, public access rights, privacy regulations, antitrust issues of access to information — all these topics are intermingled, and have to be considered together. They are bound to each other even though they sometimes have divergent approaches, but there remains one final question: How do we define rights in information versus the public domain?

If we take this approach as a new axiomatic way of understanding copyright, then the looking glasses of lawyers have to be changed. What is necessary now is to reform copyright law in Information’s Image.¹⁷⁵⁹ Traditional copyright thinking

¹⁷⁵⁶ See: Dölemeyer, Klippel (1991): 185, 198 ff.

¹⁷⁵⁷ See: Wersing (1973): 35 ff; Steinmüller (1993): 198 ff; Wiebe (1997): 93, 99 f.

¹⁷⁵⁸ See: Druey (1995): 3 et seq.

¹⁷⁵⁹ This wording is a reference to Jessica Litman’s fabulous article “Reforming Information Law in Copyright’s Image”. (Litman (1997): 587.)

is still using the old philosophical concepts of 19th century. As copyright law has been an area taught and practised by a small circle of experts, it became self-referential, autopoietic, only fixed upon itself, unable to move. The world changed — but not the copyright lawyers. The philosophical concept remained unchanged, although the rest of the world was totally changed. This was ok so long as copyright only dealt with the protection of fine arts. But at least with the inclusion of software and databases in copyright law things changes. Wide parts of our society are now affected by copyright; wide parts of industry are now affected by copyright. The shock for traditional copyright lawyers was apparent when EFF and others protested against DeCSS decisions. As the U.S. Copyright Registrar started at this conference, it was astonishing for her that people discussed these issues so broadly and vividly. But she seemed to have the impression that this broad interest was a mistake, a mere accident.

VI.2 General Principle: Freedom of Information

The historical considerations which I tried to develop above lead as well to a different understanding of the concept of copyright law as such. It is not mandatory to interpret copyright protection broadly (and vice versa, exemptions in copyright as narrowly tailored) exceptions. The general rule above any intellectual property is freedom of information. This meta-rule determines that any information can be used by everybody for free. In Germany, we have a nice folk song for that issue: “Die Gedanken sind frei.”. Thoughts, content, ideas, expressions are open to be utilized, integrated, altered by anyone.¹⁷⁶⁰ The view that knowledge, content, thoughts are common heritage of mankind is not regulated in any act. But is a general view which is underlying our legal regimes. The fact is nowadays recognized at least in the area of law and economics that information is a public good which is by its nature on-exclusive.¹⁷⁶¹

That can be seen taking into consideration the distinction between ideas and expression. It must be vexing for traditional copyright lawyers that they have been unable to find a workable borderline between the free use of ideas and the protectable expressions. Centuries have passed with attempts to define these terms; but as the discussion on the protectability of show formats has demonstrated, no solution was found. This difficulty has to do with the relationship between copyright law and information law. The idea of free ideas in copyright —only relates to the meta-concept of information law that information is the common heritage of mankind and thus free to be used by everybody.

VI.3 In Dubio pro Libertate

This approach leads to a different interpretation of copyright law. As Michael Fey has stated, “*copyright protection exists primarily for the benefit of the public, not the benefit of individual authors*”; the aim of copyright is regarded “*to ensure*

¹⁷⁶⁰ See: Druey (1997): 79 ff.

¹⁷⁶¹ See: Pindyck, Rubinfeld (2001): 645; Elkin-Koren, Salzberger (1999): 553, 559; Benkler (2000): 2063, 2065 ff.

the creation of new works”¹⁷⁶² This relates to the Copyright Clause of the U.S. Constitution: the progress of science is promoted by securing “*for limited Times to authors [...] the exclusive Right to their [...] Writings*”¹⁷⁶³.

Copyright is an exception which needs further justification. The statutory act of reducing public domain in favour of a long and extensive copyright protection can only be made where exceptional circumstances justify that step. This is the case where a high level of originality and creativity is embodied in a specific work. Only where a certain expression has individuality and represents some creativity, an attribution of exclusive rights under the copyright regime be justified.¹⁷⁶⁴

But apart from that, it was a violation of informational justice to grant a 70 years p.m.a. protection of the “*kleine Münze*” — even for software, photos and databases. This extension of copyright law to elements which resemble the Feist-ruled U.S. criteria of “*sweat of the brow*” is a product of recent EU legislation during the last 10 years. No scientific research, no economic analysis has been made before in Brussels; everything is only aimed at immediately impressing EU lobbyist groups, especially arising from the producing area.

These considerations do not only influence the interpretation of originality requirements. In the same way, they determine the question how the regulations on public access in copyright law should be interpreted. Traditional copyright lawyers often try to interpret these rules as “*exceptions*” compared to the general rule that copyright owners have the full control of the exploitation.¹⁷⁶⁵ However, this view is incorrect. It has to be reinterpreted in the light of “*In dubio pro libertate*”. Exemptions in the public interest are not “*exceptions*” to the general rule that works are copyrighted. They are limitations in favor of fundamental rights such as freedom of the press, public access or the necessities of research.¹⁷⁶⁶ Even private copying has a constitutional background, as it protects the right to privacy against rights owners who want to control the dissemination of their works in private houses. As the limitations are no “*exceptions*,” there is no need to interpret the exemptions narrowly. Instead, a balance between the different rights involved has to be made in interpreting the exemptions. This attempt to find the optimal way of combining the interests of rights holders and users very often leads to a broader interpretation of exemptions taking into consideration the general principle of free use as it has been stressed in several decisions for the German Federal Supreme Court.¹⁷⁶⁷

¹⁷⁶² See: Frey (1998): 959, 1001.

¹⁷⁶³ US Constitution, Art. I, § 8, cl. 8.

¹⁷⁶⁴ See: Similarly Litman (1990): 965 et seq.

¹⁷⁶⁵ See: Aoki (1993). 1. Aoki has demonstrated the negative effects of the tendency to narrow the public domain by the extensions of exclusive rights in intellectual property law.

¹⁷⁶⁶ It is interesting to see that Art. 5 of the InfoSoc Directive is titled “*exceptions and limitations*”. The EU legislators left the question open for discussion whether the exemptions in the Directive are “*exceptions*” or “*limitations*” (similarly Recital 19 of the Directive).

¹⁷⁶⁷ See the German Supreme Court (Bundesgerichtshof), Decision of 20 January 1994, Computer und Recht 1994, 275 — Holzhandelsprogramm.

4.5 Business, Technology, and Law — Interrelations of Three Scientific Perspectives on DRM

*Johannes Ulbricht*¹⁷⁶⁸

Abstract: Technology, law and economics influence each other reciprocally at DRM, so that it is practically impossible, to make scientific statements on DRM from the point of view of one of these disciplines, without basing them on premises from the other disciplines. That makes systematic and purposeful further development of DRM difficult — progress made in one discipline runs the risk of being devalued by further developments in the other disciplines. Therefore the question poses itself of how the different scientific disciplines can be delimited from one another, so that reciprocal transfer of preliminary work between them is facilitated. On this a proposal is to be made below with reference to practical examples.

I The Problem: DRM as an Interdisciplinary Subject

The subject of DRM is — as indeed can also be seen from the organisation of this book — usually considered either from a technical, an economic, or a legal viewpoint. One can naturally just as well approach the subject from a political–science or social–science point of view. Well, that is in itself nothing special — there are many subjects where that is the case. However, what is unusual about the subject of DRM is that it is difficult to make binding statements on this from the standpoint of an information scientist, an economist or a lawyer without at the same time also dealing with other scientific disciplines or at least taking relevant premises as the basis. When as a law student I dealt some years ago with the subject of DRM for the first time, I found that I was incapable of formulating legal statements without at the same time basing them on premises pertaining to the technical nature of the DRM system or regarding the economic transactions made possible by it. And what was even worse — the legal theses concerning DRM were as regards their statement content completely dependent upon these economic and technical premises.

For example, it was impossible for me to deal from a legal point of view with the problems of a possible violation of the freedom of action of the users and their privacy by DRM systems¹⁷⁶⁹, without in this case assuming certain premises with regard to the technical architecture of a DRM system. A DRM system, the technical basis of which is primarily cryptography, has, for example, with regard to a possible violation of the freedom of action and privacy of the users a quite different danger potential than a DRM system that is based primarily on watermarks. For a system based on cryptography can restrict and regulate the freedom of action of the user also in his private life. A system based solely on watermarks, on the other hand, can at best help to comb through public spaces such as the Internet in search of pirate copies. It can, however, not prevent

¹⁷⁶⁸ Michow Rechtsanwälte.

¹⁷⁶⁹ Cf., regarding this set of problems, Bechtold (2002): 138; with further names as well as Dix (2002); *Bygrave* within this book on page 418.

copying as such, as long as the copies remain in the user's non-transparent private domain and do not appear in public. Therefore this subject area cannot be legally assessed unless the preliminary (technical) question of what real danger potentials the technical system creates for the freedom of action and the privacy of the users has been clarified. Unfortunately, this preliminary technical question is in turn dependent upon a legal (or at least ethical) preliminary question, namely upon the question of to what extent the freedom of action and the privacy are worthy of being protected and/or have been legally protected and when to this extent a violation is deemed to have occurred. As one can see, technology and law are inseparably enmeshed in this case and cannot be examined in isolation but only together.

The economic aspects must always automatically also be considered equally inseparable. To stay with the above example — the question of a possible violation of freedom of action and privacy can only be answered when the economic interest situation has been clarified. If the economic incentives for the violation of these objects of legal protection are great, the legal assessment will be different from the situation in which the market forces themselves already ensure that these user rights are respected. That can, for example, depend on the extent to which a DRM system has a *de facto* monopoly position in the market or must compete for the favour of the users with other DRM systems. In the latter case, it can be assumed that a relatively strong economic motivation for user-friendly (and hence also data privacy protection-friendly) system design prevails. Also the technical danger potential of a DRM system cannot therefore be analysed in isolation from these basic economic conditions.

The example shows that it is difficult on the subject of DRM to concentrate solely on the economic, technical or legal aspects without of necessity having to simultaneously deal also with the other scientific disciplines. To put it in a slightly exaggerated way — there are no legal statements on DRM in itself but only legal statements on a quite particular DRM system which is clearly laid down in its technical and economic structure. While this finding almost drove me to the brink of despair during my time as a student, I then later drew the consequence from it for my dissertation by consulting an economist and an information scientist as second experts who gratifyingly were both willing to support me, the lawyer, in my interdisciplinary project.

The basic problem remains that during the analysis of the subject complex of digital rights management every academic discipline yields merely relative concepts which relate to premises from other academic disciplines and seen by themselves are without any force of expression. The whole interdisciplinary concept system in connection with DRM consists of relative variables relating to one another without any identifiable fixed point. Whoever talks frequently about the subject of DRM, will perhaps just like me have had the experience that each person involved in the conversation started from different basic assumptions concerning the technical, legal and economic facts about DRM, which in each case they saw as being something that goes without saying and the subject of which was hence not raised so that the misunderstanding only becomes apparent after some time.

This reciprocity of the various disciplines entails marked disadvantages — for the technical further development of DRM systems one must bear the basic economic and legal conditions constantly in mind. If, with regard to these basic conditions, false premises were assumed or if these basic conditions change in an unforeseen way, all investments for the further development of the technical system can be devalued. The same applies to the other disciplines — neither can an economic cost calculation be set up, in the case of DRM, in isolation from the basic legal and technical conditions, nor can the real effect of a legal norm be forecast in isolation from its economic and technical framework. That results in further development of DRM systems which is scientifically well-founded and thoroughly cost calculated with regard to expenditure and effect currently appearing virtually impossible. This applies both with regard to the further development of the technical system and to the legal formulation of licence agreements and other agreements as well as with regard to the further development of the business models.

A further disadvantageous consequence of this reciprocity is that a clear division of tasks between the various disciplines is no longer made. This can be illustrated particularly well with reference to the example of the legal provisions for the protection of copy protection technology — in this case the basic outlines of legal framework were already sketched by the two WIPO treaties — WIPO Copyright Treaty (WCT) and WIPO Performances and Phonograms Treaty (WPPT) — in 1996 which have meanwhile been incorporated at the European level into Directive 2001/29/EC of the European Parliament and of the Council of May 22, 2001 (“Directive on Copyright in the Information Society”)¹⁷⁷⁰. That directive will in turn be incorporated into German law by the “Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft” (= Act on the Governing of Copyright in the Information Society), by which the German Urheberrechtsgesetz (Copyright Act) will be amended. In Art. 11 WCT and Art. 18 WPPT there are regulations for the prevention of the circumvention of technical copy protection devices. According to Art. 11 WCT, the contracting states undertake to ensure “*appropriate legal protection and effective legal remedies against the technological measures which are taken by authors in connection with the exercising of their rights and which restrict actions with regard to their works which are not allowed by the authors in question or are not legally permitted*”. Therefore technological measures are only protected if they are effective. As a result of this requirement, easily avoidable technological measures are to be excluded. For the legal examination of whether this legal provision is applicable in a specific case, in advance a purely technical preliminary question must therefore be clarified, namely the question as to whether a certain technological measure is effective or not. Now lawyers are, however, not as a rule qualified to answer such questions. And also the function of this legal norm is not actually legal, but technical — civil law provisions generally have the function of dividing up the decision-making power between different players. The legal question of who holds the copyright to a specific work, is therefore the question of who may

¹⁷⁷⁰ See: Bechtold (2002): 211ff.

decide whether the work is, for example, to be duplicated or published. Art. 11 WTC, on the other hand, occupies itself, however, unlike other copyright norms, not with an issue of the distribution of decision-making power, but what is rather involved, is legally strengthening the technical copy protection in its way of acting specified by technology. The law therefore attempts to perform the same tasks as the technology or even to compete with the technology in the performance of these tasks. The disadvantageous result of this absence of a clear division of tasks between technology and law could, for example, be that simple recourse to legal protection leads to the technical copy protection no longer being adequately further developed. Investments in an improvement of the copy protection technology could prove uneconomical, if, besides the technology as a competing alternative, there are legal claims. Then the law inhibits the development of functioning copy protection technology, instead of promoting it¹⁷⁷¹.

A lot of other examples can be quoted of the disadvantages resulting from the fact that a clear distribution of tasks is no longer effected between the different disciplines any longer: a fear which is frequently dealt with as a subject in connection with DRM is that free material from the public domain will become increasingly copy-protected and hence only accessible for a charge and/or that the limits and facts relating to permission of copyright law by the de facto power of the copy protection technology will be deprived of their practical meaning. What these fears — no matter whether one considers them justified or unjustified — in essence involve is the fear that the distribution of decision-making power with regard to the question of whether and how certain contents can be used factually, will increasingly no longer be effected by the law but by technology and that it will hence de-democratised, and that therefore the technology could take over the tasks of the law¹⁷⁷². This, too, would be a disadvantageous consequence of an unclear distribution of tasks between technology and law — if the law no longer performs its actual task of clearly and predictably defining the contents and the limits of the copyright law, that task will be increasingly performed by technology.

The problems can surely be attributed in part to the fact that so far only little practical experience has been gained with DRM. Anyone dealing scientifically with DRM is, therefore not yet dealing with an existing system, the advantages and disadvantages of which can be observed in actual practice, but with untried prototypes which, for their part, are still the direct result of scientific work. In a similar way to what has happened to Internet law and e-commerce, the distribution of tasks between the various disciplines will become more clearly delineated in the course of time. Here, too, only a few years ago there was a lack of clarity as to which questions were to be answered by which discipline. By now a relatively smooth interaction has evolved. Nevertheless it would be desirable for the disciplines to already be clearly delimited from one another now, since, as a result, more systematic and result-orientated work on the subject of DRM would be made possible and many misunderstandings could be

¹⁷⁷¹ Cf. on this Ed Felten's Web site: <http://www.freedom-to-tinker.com>.

¹⁷⁷² See: Kuhlen (2002).

obviated. By means of a clearer distribution of tasks it would also be possible to avoid the results of research — as at least according to my observations currently frequently happens — therefore being quickly overtaken by reality and rendered obsolete, because the basic conditions in the other scientific disciplines change. In order to work out how, in order to avoid such problems, a meaningful division of the tasks between the academic disciplines could look, the reciprocal effects between economics, technology and law are to be given closer specific consideration below.

II Reciprocal Effects between Economics and Technology

The market for DRM-protected contents is quite fundamentally distinct from other markets due to the fact that it did not emerge alone but must first be artificially created. While the market is in itself a social mechanism for the distribution of scarce goods, the scarcity of the digital data is first generated artificially by the copy protection technology. The market place for digital goods exists only with cryptographic city walls (outside of those city walls there is what one could call a land of milk and honey). The limits of what is technically possible therefore also limit the area in which one can consider digital contents as scarce goods from an economic point of view — if copy protection, for example is regularly cracked after a certain length of time, the contents can only be treated as economically scarce goods on the market during that restricted time span. A central task of technology from an economic standpoint is therefore to make digital data artificially scarce in this way to make them tradable products. If this were the only task of technology, the interrelations between economics and technology would be relatively clear and well ordered — one could then cost calculate economically with DRM-protected contents as with any other goods, would, however, have to take into account the restrictions of the technical system which lead to the goods gradually losing their value with the increasing dissemination of pirate copies. For example, similarly in the entertainment software sector, the fact that a computer game as a rule is saleable as a full price product only for a relatively short length of time after its appearance is included in the economic cost calculations. Therefore that sector has developed business models which take the drop in scarcity due to pirate copies into account by putting its money on a price-wise graduated second and third evaluation. Such a role of copy protection technology as a guarantor of scarcity in the market can be covered without any problems within classic economics, so that one can put a relatively exact figure on the economic benefit of the copy protection on the basis of the additional sales made possible by this. Therefore on this basis one can also calculate without difficulty as to whether it is worth buying “additional scarcity” by investment in copy protection technology.

The role of technology in the case of DRM, however, is known to go beyond merely making copy protection available. Among other things, a DRM system also includes an infrastructure for marking and identifying information as well

as an infrastructure for electronic trading in rights to copy-protected works¹⁷⁷³. These system components do not exist independently of one another, but must of necessity relate to one another. Since the rights to digital works can only be traded to the extent that they can be protected by the copy protection and that they can be marked and identified. It would surely not make much sense, in a language definition for electronic trading in copyrights, for example, to provide language elements for the acquisition of rights to samples and similar integral parts of the works, if such integral parts of the works can be neither secured by copy protection nor be identified by the system as independent objects. The technology therefore supplies an infrastructure which defines overall to what extent works protected by copyright are tradable as products or not. That the technology has this function is not new and should not be likely to pose any special problems — also in the case of trading with tangible data media such as gramophone records or CDs the technical infrastructure defines the tradable product. In that way, the technical infrastructure provides certain constant parameters for the economic cost calculation. The distribution of tasks between economics and technology is clear to that extent — economics provide the technology with target specifications as to which contents are economically valuable and therefore worth protecting. Economics provide the technology, in addition, with target specifications as to which utilisation actions are of such great economic significance that it is worth suppressing them (therefore at what stage of the utilisation of the contents barriers incurring costs can be appropriately constructed). Technology in turn sends a feedback to economics as to how much protection is possible at what price.

What now, however, disrupts this division of tasks between economics and technology is the fact that the technical system is more than only a neutral infrastructure, within the framework of which economic acts are performed. It is, moreover, itself also a product which is developed to meet a quite specific demand. DRM systems are currently mainly financed and used by the holders of the rights. The configuration of the DRM systems will therefore be primarily oriented to the needs of the holders of rights. DRM systems protect mainly what for the direct financiers of these systems — that is, in the present economic situation the holders of the rights — is of great economic significance. Moral rights or copyright-related barriers in the general interest will presumably tend rather to be neglected¹⁷⁷⁴. That could, for example, be different if the artists themselves marketed their works directly and in this case bore the cost of the use of the DRM systems. Then there would be an economic incentive for the developers of the DRM systems to cater for the intangible needs of their customers and also to illustrate moral rights in the system.

The German draft for the reform of the Copyright Act (government draft) likewise goes along with this thesis and assumes that the interests of the public in the preservation of certain areas of freedom such as the private copy and other copyright barriers are not adequately taken into account in the architecture of

¹⁷⁷³ See: Bechtold (2002): 23 ff.

¹⁷⁷⁴ See: Kuhlen (2002).

the DRM systems. The purpose of the German government draft is, among other things, the implementation of the already mentioned WIPO treaties WCT and WPPT as well as EU Directive 2001/29/EC which is based on them. In Art. 95 b it provides for the public's being able to enforce these areas of freedom protected by copyright through the courts, if they are not illustrated in the DRM system. This is based on the legislative assumption that the copyright balance between freedom of information and control of information can be disrupted by the DRM systems, as they primarily make allowance for the interests of those players who finance the system and will be blind to the contrary interests of other players. Whether this thesis of the legislators will prove true in practice, remains to be seen. It is, in any case, at least likely that the design of the system architecture will be influenced by the basic economic conditions under which the system is shaped and further developed. In Germany there is a proverb for it, "Whoever pays, acquires".

The technical problems must therefore not be seen in isolation from the basic economic conditions under which the technology is conceived and further developed. This can be very nicely seen from the example of exchange marts — in the public perception problems posed by this are mainly regarded as technical problems — it is quite definitely already a platitude to say that the technology on which the exchange marts are based is "uncontrollable". Here an important aspect is neglected, namely the aspect of the basic economic conditions and incentives due to which this technology is developed. As exchange marts are financed exclusively by income from advertising, it is decisive for the survival of an exchange mart, at least at the outset, to reach the largest possible number of users quickly. Therefore exchange marts, at least during the early phase of their existence, are orientated as regards system design exclusively to the interests of the users and the interests of the artists and other holders of rights are neglected. During this early phase, it is also only on certain conditions possible to exert pressure with the threat of having the exchange mart shut down by legal action. For, at that stage, neither much time nor much money has been invested in its set-up so that no great economic loss would be incurred by the operators as a result of a shutdown. If, on the other hand, once an exchange mart has become well-known, the interest becomes greater in catering not only for the needs of the users but also for the interests of the artists and other holders of rights — while, for example, Napster once concluded the famous deal with Bertelsmann, Kazaa is trying, by offering DRM-protected contents, to be a potential partner of the holders of the rights.

An important aspect of the exchange mart problems which is easily overlooked in the case of a purely technical view of the matter, is therefore the fact that it is currently relatively easy to finance illegal offers on the Internet via income from advertising. If it were possible to eradicate this economic incentive by legal means or one could establish opposed economic incentives, it would in that way be possible to indirectly influence the shaping of the technical infrastructure.

Therefore one can say, with regard to the delimitation of the task areas of economics and technology from one another, that the technical infrastructure

therefore creates, on the one hand, a framework within which an economic cost calculation for the digital data first becomes possible. On the other hand, the technical infrastructure itself is characterised by economic incentives. As a result of this, it is in particular also determined whose interests are taken into account during the design of the infrastructure and to what extent. Therefore it is an economic question as to how digital data are sold most profitably in a given DRM system. It is likewise an economic question of by what economic incentives a particular configuration of the DRM infrastructure can be brought about or what the economic causes of a faulty development during the shaping of that infrastructure are. It is, on the other hand, a purely technical question of how the economic interests of a player are best implemented in the infrastructure or, however, the infrastructure is shaped in such a way that unnecessary conflicts of interests between the players are largely avoided. The economics defines the goals, the technology finds the way there. However, the economic target specifications, on their part, are in turn influenced by what is technically possible and meaningful.

III The Role of the Law

The law has a double function — on the one hand it is to ensure a certain balancing: of the interests between the players involved. It therefore compensates for a preponderance of economic or technical (or other) power — the legal struggle of the holders of rights against the exchange marts is an attempt to correct the (technically induced) position of dominance of the exchange mart operators by legal means and to obtain an own position of power, in order to have a decisive say in the design of the technical infrastructure. The legal struggle is above all of interest for those persons who cannot enforce their interests either economically (that is, for example, by buying up exchange marts, as happened in the case of Napster) or technically (e.g. by the spreading of viruses or MP3 fakes). But the law brings about, besides the partial compensation of the *de facto* power situation, also something else, namely a permanent fixing of these power relations — by the legal offsetting of interests a stable, reliable state is reached. Therefore, whoever can completely enforce his interests solely on the basis of his technical and economic predominance, can also benefit from securing himself legally. In this way he obtains a certain planning certainty.

This second function of the law, the creation of calculable and reliable basic conditions, is highly problematic especially in the case of DRM — since the technical and economic starting position on which the legal provisions are based and which they assume (consciously or unconsciously), change extraordinarily quickly particularly with DRM and will probably also continue to do so in the foreseeable future. That is not only due to the lightning further development of digital technology, but also to the thus induced change in the public's reception habits, which in turn causes the emergence of new business models. However, the law always starts from implicit premises with regard to reality and functions in the intended way only as long as these premises remain the same. Legal

provisions generate dysfunctional effects as soon as the reality on which they are based changes in an unexpected way. A good example of this is the legal term of the private copy — this term is based on the implicit premise that everyone to a limited extent can produce analogous copies within his household area and can occasionally pass them on to persons he knows. This premise was perfectly correct at the time of the coining of this legal term in the 1960s, since the tape recording technology at that time permitted just that and not more. The private copy was, at that point in time, an insignificant dark niche into which it was not worth casting any light. Probably this premise was at that time not even consciously perceived, but taken for granted. After all, the triumphal entry of digital technology and the changes induced by it were not foreseeable at all at that time. Without the legal ruling in itself having changed, it now has, in a digital environment, completely unforeseen and unintentional effects going as far as the attempt at a legal justification of exchange markets. By means of the digitisation of the mass media the duplication and dissemination possibilities for everyone have been enormously expanded; the insignificant dark niche of the private copy has meanwhile grown into a huge space in which visibility is as poor as ever.

But not only legal concepts such as the private copy, but the conceptual basis of the copyright system as a whole is being questioned by further technical development — the applicable copyright law is based on the basic assumption that the extent of the utilisation, liable to remuneration, of works protected by copyright can be measured on the basis of the number of existing numbers of original copies of the works and therefore starts not from the use but instead from the duplication and dissemination of copies of the works when it is a matter of defining facts of the matter requiring approval and remuneration. This basic assumption is correct for the analogue area, but for the digital area it is simply incorrect — the digital duplication and dissemination of works protected by copyright is not only an everyday process, but in many cases also an unavoidable one. Examples of such unavoidable copies are the ephemeral copies on proxy servers and in the working storage, the back-up copy as well as duplication for the use of the data in a different format. Not every copying process in the digital area has a detrimental effect on the intangible or economic interests of authors. In reverse there are processes which do in fact manage without any duplication but which, nevertheless lead to a de facto loss of the control over the work under copyright law, such as the sale of second-hand books, phonograms and other data media for example by amazon and ebay. It can therefore be stated that the conceptual and economic interest of the author in the control of access to the work in the case of digital media is not to be equated with a check on the duplication control. In the case of analogue media, by contrast, control of utilisation of the work and control of the duplication of the work were largely congruent. The economic and also the intangible aim of copyright law which is to provide the creator with control of access to the work is increasingly moving away from the legal protection area, namely control of the duplication of the work. In the digital area it is no longer a matter of possessing an original copy of the

work, it is a matter of access to the incorporeal contents in themselves. It appears probable that this discrepancy between the actual aim of copyright law and its factual protection area will become increasingly greater with continued further development of digital technology with dysfunctional effects as a disadvantageous consequence.

Even if legal provisions start from the physical hardware, they can at best function in the analogue area, but in the digital area they inevitably overshoot the intended regulatory mark — since, in the case of the digital technology, the physical data medium and the contents stored on it are logically separated from each other. Data and contents are in the case of digital technology, differently from analogue technology, separated from each other at two logically completely independent levels. Hardware stores merely data, but not directly contents as such. Therefore, in the case of digital technology, the hardware does not permit any conclusions to be drawn as to the type or quantity of the contents. And so it does not, for example, make any sense, to levy lump-sum charges under copyright law to cover private copies onto digital hardware. It cannot be demarcated on which hardware charges are to be levied and on which none are to be levied. Even the premise that whoever acquires the hardware, also makes private copies on it, is no longer correct. Since the hardware can just as easily be accessed via the Net, one no longer needs to place it in one's own home in order to use it for private copies¹⁷⁷⁵.

It can be seen how sensitive legal provisions are to changes in the technical and economic environment. The consequence of this should be to restrict oneself, when carrying out the legal formulation, to the actual task of the law which is namely the definition of a calculable and durable contents-related consensus between the players involved. The law should only define the goal and objectives. Finding the way to this goal should be left to economics and technology. Otherwise not only over-regulation with numerous hampering details threatens to develop, above all dysfunctional effects threaten to emerge as one can easily see from the examples mentioned.

IV Result

The relationship between technology, the law and economics can — in a somewhat simplified way — be put into a nutshell in the following way: technology imparts to whoever controls it possibilities for action and thus endows him with *de facto* decision-making power. By comparison, economics deals with how, as a player, one makes the best possible use of this decision-making power. At the same time, economic criteria also decide how the technology is further developed. The law, on the other hand, stabilises and corrects the distribution of technical and economic power and makes statements as to how the decision-making power should be distributed.

¹⁷⁷⁵ On page stated; see: Kreile (2002).

4.6 The Present and Future of Digital Rights Management — Musings on Emerging Legal Problems

*Stefan Bechtold*¹⁷⁷⁶

Abstract: This article presents a roadmap of emerging legal problems in the area of Digital Rights Management (DRM). It argues against adopting fundamentalist viewpoints in the DRM policy debate. In particular, DRM technology is much more flexible than many DRM critics acknowledge. The article covers various problems that are less frequently discussed in legal and policy circles. It analyzes the relationship between DRM, fair use, and innovation, using rights locker architectures, dynamic DRM systems, the Creative Commons project, DRM technology license agreements, and security research as examples. It addresses the alleged dichotomy between DRM and copyright levy systems as well as the implications of DRM for privacy protection. By analyzing various technology platforms, it describes the implications DRM has for competition in platform markets as well as in complementary aftermarkets. Finally, the article assesses recent efforts to standardize DRM technology, both by the private sector (in particular TCPA and Palladium), and by the legislature.

I Introduction

Digital Rights Management (DRM) promises to offer a secure framework for distributing digital content (music, video, text, rare data etc.). DRM enables an electronic marketplace where previously unimaginable business models can be implemented. At the same time, DRM ensures that content providers — particularly copyright owners — receive adequate remuneration for the creation of the content that is distributed over the DRM system. And so, copyright owners lived happily ever after.

So goes the DRM story told by DRM disciples. If one listens to DRM opponents, however, the story sounds very different. In the United States and in Europe, much has been written about how DRM privatizes and replaces copyright law,¹⁷⁷⁷ how it undermines copyright limitations,¹⁷⁷⁸ threatens the interests of users and the public at large, inhibits creativity and innovation by unjustly extending intellectual property protection,¹⁷⁷⁹ how the law and economic anal-

¹⁷⁷⁶ Research Assistant, University of Tübingen Law School, Germany; Fellow, 2002–2003, Center for Internet and Society, Stanford Law School, USA. The author is grateful to Ross Anderson, Robert Gehring, Brian Hemphill, Kurt Jaeger, Lawrence Lessig, Yuko Noguchi, Roy Pfitzner, Graeme Proudler, David Safford, Tomas Sander, and Florian Wagner for helpful comments.

¹⁷⁷⁷ See: Lessig (1999): 130, 135; Gimbel (1998): 1683–1684.

¹⁷⁷⁸ See: Koelman, Helberger (2000): 189–192; Cohen (1998): 472–473; see also: Guibault (2002).

¹⁷⁷⁹ See: Lessig (2001). See also: The articles from the Duke Conference on the Public Domain 2001 in 66 *Law and Contemporary Problems* 1–483 (2003); Elkin–Koren, Netanel (2002).

ysis by DRM proponents is flawed,¹⁷⁸⁰ and how anti-circumvention regulations are overbroad and undermine fair use.¹⁷⁸¹ And so, this version of the DRM story goes, at the dawn of the third millennium, the world of creativity and cultural production collapsed due to an unfortunate conspiracy of huge commercial conglomerates and biased legislators.

As with many controversial stories, both versions of the DRM story have elements of truth to them.¹⁷⁸² However, as with many controversial stories, both also include elements of exaggeration and, sometimes, even falsity. Although the author shares most of the mentioned concerns about DRM,¹⁷⁸³ this article does not directly address them. Rather, it focuses on some aspects of DRM that are less frequently discussed in legal and policy circles, either because they have emerged only recently or because they are not as well publicized. Thereby, the article attempts to add several problems to the existing myriad of DRM-related problems.

At the same time, the article attempts to show that it is often futile and sometimes counterproductive to condemn DRM altogether. Digital rights management offers many tools by which some of the problems raised by DRM opponents can be solved. In particular, DRM technology is much more flexible and plastic than some DRM critics acknowledge. As understood in this article, “digital rights management” is a general term for a set of intertwining technologies that may be used to establish a secure distribution channel for digital content. Such technologies include encryption, copy control, digital watermarking, fingerprinting, traitor tracing, authentication, integrity checking, access control, tamper-resistant hard- and software, key management and revocation as well as risk management architectures.¹⁷⁸⁴ All these technologies are used to *enforce* certain policies. In addition, most DRM systems also include certain technologies that enable the machine-readable *expression* of such policies, in particular

¹⁷⁸⁰ See: Cohen (1998).

¹⁷⁸¹ See only: Samuelson (1999): 548–549. For some proposals to bring anti-circumvention regulations in accordance with copyright limitations, see: Burk, Cohen (2001); Burk (2003); see also: Foged (2002).

¹⁷⁸² Actually, a third version of the DRM story exists. According to this version, all the policy discussions about DRM are essentially futile as it is either technically impossible to design a secure DRM system (see: Kelsey, Schneier (1998): 2) or unrealistic to expect DRM to eradicate P2P file sharing networks and other so-called “darknets” (see the Article from *Biddle, England, Peinado, Willman* within this book on page 344). While the author agrees with the second argument, the first agreement ignores that DRM is not only about technological protection. Although it is impossible to design a DRM system that is 100% technologically secure, DRM may still provide a very high level of security, as various technological and legal means of protection (including protection by copyright law, anti-circumvention regulations, usage contracts and technology license agreements) are intertwined in advanced DRM systems. For an analysis of the implications of these intertwining means of protection, see: Bechtold (2002/2003a). In the following, the article assumes that DRM systems are at least partially effective in protecting digital content.

¹⁷⁸³ See: Bechtold (2002/2003a).

¹⁷⁸⁴ See: Chapter 2 *Technological Aspects* within this book.

rights expression languages (RELS) and metadata.¹⁷⁸⁵ The specific technologies used vary from DRM system to DRM system. Depending on the particular combination of these technologies, the policy implications of various DRM systems vary greatly as well.

Instead of taking DRM systems as given constants that are exogenous to the policy process, this article joins an emerging scholarship which asks how DRM systems could be altered in a value-centered design process so that important policy and legal values are preserved.¹⁷⁸⁶ The article does not attempt to provide answers to all the questions raised. Rather, in providing a roadmap of emerging legal problems, it attempts to point to various aspects of the DRM debate that deserve further analysis and discussion. For this purpose, the article may sometimes oversimplify or exaggerate certain technological trends and possibilities as well as speculate about future developments. This is done, however, to stimulate further discussion about what is possible with DRM systems and to scrutinize various DRM characteristics that have been taken as given, unalterable facts hitherto.

The article proceeds as follows. In section II, four aspects of the interrelation among DRM, fair use, and innovation, which are under-represented in current DRM policy discussions, are described. Section III addresses the alleged dichotomy between DRM and levy systems. Section IV touches upon the impact of DRM on privacy protection. Section V analyzes the implications of DRM for competition in the DRM-protected platform market itself and in complementary markets. Section VI assesses recent efforts by the private sector and by legislatures to standardize and mandate DRM technology. Section VII concludes the article.

II DRM, Fair Use, and Innovation

Much has been written about the impacts DRM has on fair use and creativity. In the following section, four areas will be described that are less frequently discussed. As this section will show, DRM may indeed impede fair use¹⁷⁸⁷ and innovation. However, there are also aspects of DRM which can be used to protect fair use and foster openness and innovation.

¹⁷⁸⁵ For a general overview of the technologies used in DRM systems, see: Bechtold (2002): 19–145; Rosenblatt, Trippe, Mooney (2002).

¹⁷⁸⁶ For other examples of this scholarship, see: Burk, Cohen (2001); Cohen (2003); Mulligan, Burstein (2002); Fox, LaMacchia (2003); Erickson (2003). But see: Felten (2003).

¹⁷⁸⁷ The use of the term “fair use” in this article is meant to cover a broad range of copyright limitations. It is not meant to describe the U.S. concept of fair use in contrast to the more detailed copyright limitations that may be found in the copyright laws of many *droit d’auteur* countries in continental Europe.

II.1 Rights Locker Architectures

With the increasing mobility of people and the increasing spread of communication networks, media consumption patterns change. Formerly, consumers were satisfied if they could listen to music on their record player in their living room. Increasingly, consumers seem to demand that they can access and use their content from any media device they own. Thereby, they could listen to their favorite music at home, in their car, in the subway, at work, in the plane or in a hotel room.

DRM technology attempts to respond to this demand. The idea is to enable consumers to access any content at any time from any device they want in a DRM-protected environment. Such a system could give consumers instant access to the entire world of information and entertainment via their computer, MP3 player, PDA and cell phone, from any place in the world.

“Rights locker” architectures are the technology that promises to make this happen. In a DRM rights locker architecture, content is no longer stored on a particular device the consumer owns. Rather, it is centrally stored on a network server. This server is also a central depository for the permissions to use content which a consumer has purchased.¹⁷⁸⁸ If, in a DRM rights locker architecture, a consumer wants to listen to some audio content on his computer, the computer does not load the audio file from its local hard drive. Rather, it sends a request (together with some authorization information) to the central server. After the central server has verified the authenticity of the request, it streams the audio file back to the computer. If the consumer wants to listen to the same content on his wireless device a few hours later, the same procedure takes place. In such an architecture, local storage of content becomes unnecessary.¹⁷⁸⁹

Rights locker architectures make digital rights portable among various platforms as permissions to use content are no longer bound to a particular device the consumer owns, but to the consumer himself.¹⁷⁹⁰ They also provide reliable backup mechanisms for such digital rights, as consumers do not have to fear to lose their rights due to hardware failures or by buying a new computer.¹⁷⁹¹ Rights locker architectures therefore provide portability and recoverability of digital rights.

While rights locker architectures will not be implemented on a wide scale in the near future, many DRM technology companies are currently working on such systems. Given the limited memory storage of many wireless devices, rights locker architectures may become of particular importance in a future where wireless devices and networks play a role comparable to the Internet as we know it today.

¹⁷⁸⁸ See: Sander (2002): 66; Feigenbaum, Freedman, Sander, Shostack (2001): 101–104.

¹⁷⁸⁹ This is an oversimplification, of course. Even in a rights locker architecture, local storage will remain important due to bandwidth limitations, high costs for streaming content in wireless networks and network outages. The article accepts this oversimplification in order to highlight a certain trend.

¹⁷⁹⁰ See: Sander (2002): 66.

¹⁷⁹¹ See: Id.

The current discussion about DRM and fair use is implicitly based on the assumption that consumers have copies of the protected content that are physically stored on devices the consumers own. Under such circumstances, it is reasonable to ask under what conditions the consumer is allowed to copy content from one device to another without the rights holders' permission; it is also reasonable to ask under what conditions the consumer is allowed to forward his copy to friends (as the copyright limitations for private copying and the fair use defense sometimes allow). These questions make sense in a world where data is physically stored on devices that are located in the realm of the consumer.

These questions become less important in a world where content is stored in a central location and only transmitted to authorized devices on demand. If all content any consumer could ever desire is available from a network server, no need seems to exist for a consumer to transfer content between his computer and his MP3 player, as both devices could download the content from the network. Why, then, should copyright law exempt such activities from copyright liability? Do rights locker architectures render any limitations to copyright protection that are based on the idea of "space shifting" obsolete? If, in a rights locker architecture, a consumer wants to recommend a video to a friend, he does not have to transmit the video file to his friend anymore. Rather, he may simply send him a link that points to the location of the video file on the central server. If the friend can download the movie from the network without problems, why should copyright law exempt copying among friends from copyright liability? What is the notion of fair use in a world where any content is available for everybody from any location at any time?¹⁷⁹²

Although it is beyond the scope of this article to provide a comprehensive answer to such questions, it should be noted that fair use will still play an important role in rights locker architectures. Among other things, copyright limitations induce positive external effects that are important for subsequent creativity.¹⁷⁹³ The justification for such limitations will also apply in rights locker architectures. Yet, the characteristics of copyright limitations may have to change in a rights locker

¹⁷⁹² Rights locker architectures make local storage of content unnecessary and challenge copyright limitations that assume the necessity of such storage. In this regard, they are similar to the challenges the GNU General Public License (GPL) is exposed to by application service providers (ASP) and web services. The GPL builds upon the assumption that software source code is distributed to programmers so that they can adapt and change the code. With both ASPs and web services, however, no need exists anymore to distribute any source or object code of computer programs. Rather, software programs are run on a central network server and are accessed through a web or another network user interface. Without the distribution of source code, the protection of the free software/open source idea by the GPL could fail. For more information, see *FSF Endorses New "GPL + Web Services" License, Requests Comment*, available at: <http://www.kuro5hin.org/story/2002/3/20/154118/890> (Mar. 20, 2002); interview with Richard M. Stallman on Slashdot, available at: <http://slashdot.org/interviews/00/05/01/1052216.shtml> (May 1, 2000).

¹⁷⁹³ See: Bechtold (2002): 330–336; Gordon (2002a): 186; Burk, Cohen (2001): 43–47. See also: Gordon (2002b).

architecture. To achieve many (but not all) of the goals of current copyright limitations, it could be sufficient to grant consumers access to the rights locker without the rights holder's permission. In such a scenario, a consumer would not be allowed to receive a copy of some content from a friend without the rights holder's permission (because there would be no need to copy), but he would be allowed to receive the content from the rights locker depository without the rights holder's permission. Fair use, in other words, would not cover the physical copy of the content, but the attached rights that are stored in the rights locker. While such an approach may not be a silver-bullet solution,¹⁷⁹⁴ it seems more than worth exploring. If the importance of physical copies disappears in a more and more networked world, copyright limitations that are based on physical assumptions may have to adapt as well.

II.2 Dynamic DRM Systems, Cumulative Innovation, and the Commons

Quite often, DRM systems are depicted as if it were in their technical nature to restrict creativity and suppress fair use. This section attempts to show why this description is partially incorrect. DRM deals with the "digital management of rights". What the characteristics and scope of these rights are is not determined by obscure technical necessities, but can be determined by technologists, lawyers, politicians — i.e. by the society as a whole. Fortunately, DRM technology is very malleable. Nothing in the "nature" of DRM requires that DRM be only used for restricting access to protected content or suppressing fair use privileges.¹⁷⁹⁵ Properly understood, DRM is a much more neutral technology than commonly acknowledged.

Dynamic DRM Systems

One argument against DRM is that it suppresses subsequent creativity. It is one of the persistent and widespread errors in the legal and even the economic analysis of innovation that creativity and innovation are a static process.¹⁷⁹⁶ Rather, both are cumulative and dynamic processes. Therefore, as any intellectual property, copyright law must ensure that by providing incentives for creativity, it does not overly restrict access to already existing works.¹⁷⁹⁷ This line of reasoning may also be applied to DRM systems. By over-protecting digital content with DRM systems, critics claim, subsequent creators are deprived of the possi-

¹⁷⁹⁴ Such a rights locker architecture that supports fair use would have to address several concerns. As Dan Burk and Julie Cohen have pointed out in a slightly different context, centralizing control over who can benefit from fair use privileges creates various institutional dangers; see: Burk, Cohen (2001): 59–65. A rights locker architecture would have to make sure that users can benefit from fair use privileges even if this runs contrary to the interests of rights holders and of the operator of the rights locker; see: id.: 60–64. Furthermore, such architecture could chill spontaneous uses; see: id.: 65–66.

¹⁷⁹⁵ For a powerful argument against the idea that technology cannot be regulated because of its innate "nature", see: Lessig (1999): 24–29.

¹⁷⁹⁶ See: Kitch (2000): 1738–1739.

bility to reuse this content. DRM systems, the argument goes, protect content in a static way and are therefore, in a long-term perspective, dangerous to innovation and creativity.

While the author agrees with the underlying economic analysis of this argument,¹⁷⁹⁸ and while it may be true that most current DRM implementations have such shortcomings, there is nothing in the “nature” of DRM that prevents it from addressing cumulative creativity and innovation. Rather, it is imaginable that DRM would provide tools to deal with cumulative and overlapping creativity.

Such a “dynamic” DRM system would have to meet two requirements. Firstly, it would have to provide a “rights expression language” in which cumulative creativity can be properly expressed. Secondly, it would have to be able to cope with the relationships among numerous rights holders of various generations. Both requirements will be described in more detail in the following.

DRM systems use so-called “metadata” to express “usage rules”, i.e. the conditions under which protected content can be used and accessed by an authorized user. So-called “rights expression languages” (RELs) enable the content provider to express a rich set of usage rules in machine-readable metadata that can be attached to the content. One of the most well-known RELs is the “eXtensible rights Markup Language” (XrML).¹⁷⁹⁹ XrML is a “general-purpose language in XML used to describe the rights and conditions for using digital resources.”¹⁸⁰⁰ With RELs such as XrML, the permission to copy, delete, modify, embed, execute, export, extract, annotate, aggregate, install, backup, loan, sell, give, lease, play, print, display, read, restore, transfer, uninstall, verify, save, obtain, issue, possess, and revoke content may be expressed in a machine-readable form.¹⁸⁰¹ The grant of these rights may be conditioned upon a wide array of circumstances:

¹⁷⁹⁷ How intellectual property law should deal with this tension is an open question. For an overview of the debate, see: Galline, Scotchmer (2002); see also: Lemley (1997). For an argument that broad patents are socially beneficial because they stimulate further innovation, see: Kitch (1977); but see: Merges, Nelson (1990). For an account of the importance of having commons for innovation, see: Lessig (2001).

¹⁷⁹⁸ See: Bechtold (2002): 334–336.

¹⁷⁹⁹ See: <http://www.xml.org>. XrML originally stems from research by Mark Steffik at Xerox PARC and is now under the auspices of ContentGuard. In April 2002, ContentGuard submitted XrML to OASIS, an XML interoperability standards consortium that plans to develop a standardized REL. Other rights expression languages include the “Open Digital Rights Language” (ODRL; <http://www.odrl.net>), the “eXtensible Media Commerce Language” (XMCL; <http://www.xml.org>), and the “eXtensible Access Control Markup Language” (XACML; <http://www.xacml.org>).

¹⁸⁰⁰ eXtensible rights Markup Language (XrML) 2.0 Specification, Part I: Primer 5, at http://www.xrml.org/get_XrML.asp (Nov. 20, 2001).

¹⁸⁰¹ For an overview, see: Id.: 13; Open Digital Rights Language (ODRL), Version 1.1, 8, 33–34, available at: <http://www.odrl.net/1.1/ODRL-11.pdf> (Aug. 8, 2002); see also: <http://www.giantstepsmts.com/DRM%20Watch/xrml20.htm>. For a more detailed description of the rights available under XrML, see: eXten-

access to and use of digital content may be restricted to certain time periods, locations, devices (for example, computers, storage media, printers, and computer displays), and to certain users. Furthermore, the number of times content may be accessed or used can be restricted. At which quality, in which format and for what purpose the content may be accessed may also be defined. Finally, the access and use may be conditioned upon the payment of a flat or a pay-per-use fee.¹⁸⁰²

Although it is beyond the scope of this article to describe RELs in detail, it is striking that most current RELs do not provide ample tools to express how and under which conditions content may be reused, altered, reformatted, modified or otherwise transformed for the integration — be it in part or as a whole — into other works. A dynamic DRM system would require an REL that would be able to manage transformative uses, overlapping innovation, and the creation of derivative works in a fine-grained way. Although there is a clear lack of dynamic REL implementations, some research initiatives have recently started to work in this area.¹⁸⁰³

Furthermore, as was mentioned above, a dynamic DRM system that manages transformative reuses should be able to cope with the relationships among numerous rights holders. If some content is reused in another work and if this process is reiterated several times, the legal relationships between all the rights holders involved can become very complex. Similar complexity results from digital works that are based on a multiplicity of existing works (the “clip-art phenomenon”). In the area of movies, operas and multimedia works, the law has developed rather elaborate mechanisms to cope with such multiplicity of rights. A dynamic DRM system, and in particular its REL, should be able to express and manage complex relationships between rights holders as well. Here again, current DRM systems often lack adequate tools to deal with cumulative creativity if a large number of creators is involved. And again, at least some ongoing research is attempting to develop such RELs and DRM systems.¹⁸⁰⁴

sible rights Markup Language (XrML) 2.0 Specification, Part IV: Content Extension Schema 7–25, available at: http://www.xrml.org/get_XrML.asp (Nov. 20, 2001); eXtensible rights Markup Language (XrML) 2.0 Specification, Part II: Core Schema 29–31, available at: http://www.xrml.org/get_XrML.asp (Nov. 20, 2001).

¹⁸⁰² See: eXtensible rights Markup Language (XrML) 2.0 Specification, Part III: Standard Extension Schema 4–37, available at: http://www.xrml.org/get_XrML.asp (Nov. 20, 2001); Open Digital Rights Language (ODRL), *supra* note 1801, at 10–14, 35–38.

¹⁸⁰³ See: Kumazawa et al. (2001) (describing a rights expression language that uses a hierarchical structure to describe cumulative innovation); Kumazawa et al. (2000); Yasukawa (2003) (describing a DRM system that deals with cumulative innovation that is able to dynamically and interactively generate reuse license agreements that respond to the individual and changing preferences of creators of both existing and new content); Yasukawa (2002). For some comments on the Creative Commons project, see: *infra* text accompanying notes 1806–1808.

This is not to say that, in a dynamic DRM system, every transformative use should be controlled and subject to a license under the aegis of the DRM system. Having unfettered areas, or commons, in the information ecology is an essential prerequisite for maximizing innovation.¹⁸⁰⁵ But even approaches that attempt to preserve openness in our information ecology could benefit from dynamic DRM technologies, as the following subsection will illustrate.

DRM, Creative Commons, and Linux

One example of how DRM components can be used to preserve openness and alternative modes of creativity is the Creative Commons project.¹⁸⁰⁶ In December 2002, the project, directed by Lawrence Lessig and based at Stanford Law School's Center for Internet and Society, started its Licensing Project. It offers licenses that allow copyright owners to easily inform others that their works are free for copying, distribution, display, performance, modification, or reuse, or any combination or subset of the usages listed. Inspired in part by the open source software movement, Creative Commons intends to create a vibrant distributed collection of works of all sorts that are the base for creative reuses and cumulative innovation.

From an abstract perspective, Creative Commons is in the business of managing "rights" in a digital way: it enables copyright owners to grant users certain permissions to use their content in certain ways (such as to re-use their work in a derivative work), but to prohibit other uses (such as to use the work for commercial purposes or to distribute a derivative work under license terms other than Creative Commons' license terms). To achieve these goals, Creative Commons uses the World Wide Web Consortium's "Resource Description Framework" (RDF) and the "Dublin Core" metadata system to express the permissions granted by copyright owners in machine-readable metadata.¹⁸⁰⁷ In other words, Creative Commons is using a DRM rights expression language in order to preserve openness and enrich the "commons".¹⁸⁰⁸

¹⁸⁰⁴ See: Kumazawa et al. (2001) (describing a rights expression language that "clarifies relation among each rights holder and relation among his/her offered terms and profit allocation to each holder"); Kumazawa et al. (2000).

¹⁸⁰⁵ See: Lessig (2001).

¹⁸⁰⁶ See: <http://www.creativecommons.org>.

¹⁸⁰⁷ See: <http://creativecommons.org/learn/technology/metadata>. For some criticism on this approach, see: Clark (2003). Meanwhile, Creative Commons metadata can be automatically included in weblogs and weblog RSS feeds by weblog authoring programs such as Movabletype and Userland's Manila; see: <http://www.movabletype.org/docs/mt26.html#creative%20commons%20licenses>; <http://manila.userland.com/creativeCommonsRssManila>. For an argument that this creates a DRM system, see: <http://doc.weblogs.com/2003/04/13#theWhateverLicense>.

¹⁸⁰⁸ Creative Commons emphasizes that it is not in the "digital rights management" business, but merely uses "digital rights description" or "digital rights expression" (DRE) technology; see: http://creativecommons.org/faq#faq_entry_3323; Lawrence Lessig, available at: http://cyberlaw.stanford.edu/lessig/blog/archives/2003_04.shtml#001067.

Another example of how DRM components may be used to preserve openness and alternative modes of creativity is the Linux kernel. This core component of the open source Linux operating system is distributed under the GNU General Public License (GPL).¹⁸⁰⁹ The Linux kernel allows kernel-level code to be added at run-time. Thereby, after Linux has booted, additional functionality, such as hardware device drivers, new system calls or support for another file system, can be loaded into the system without rebooting the system or recompiling the kernel. Typically, such “loadable modules” use and incorporate kernel functions and data structures and may therefore be a derivative work of the Linux kernel.¹⁸¹⁰

Section 2 b) of the GPL demands that all derivative works may only be distributed under the conditions set forth by the GPL. Thereby, the “viral”¹⁸¹¹ GPL prevents proprietary modules from being loaded into the Linux operating system. From an open source perspective, this provision of the GPL has an important purpose: it attempts to keep as much software components open and free from proprietary control as possible.¹⁸¹²

It objects to characterizations of its Licensing Project as a DRM project. This results from a different use of the term DRM. In the view of Creative Commons, the term “digital rights management” encompasses technologies that *enforce* certain policies, while DRE encompasses technologies that *express* them. This author agrees that the distinction between policy enforcement and policy expression is a very important one. The legal and policy implications of both sets of technologies are very different. Regularly, policy enforcement technologies raise much more concerns than mere policy expression technologies. Yet, as was described *supra* text accompanying note 1785, as opposed to Creative Commons, the author adopts a more neutral understanding of the term DRM which encompasses both policy enforcement and policy expression technologies. According to this terminology, “DRE” is just a subset of technologies that belong to the more general term “DRM”. This is not to say that Creative Commons provides a full-fledged DRM system with access control, encryption and so on. However, as this subsection attempts to show, Creative Commons uses some DRM technologies such as rights expression languages and metadata. This illustrates that, properly understood, DRM is a neutral technology that does not *per se* violate the goals of Creative Commons. Of course, most of the current commercial DRM *implementations* run counter to the goals of Creative Commons. But this discrepancy is not inherent to DRM *technology*. For a related argument that open source software does not run counter copyright law, but rather depends on it, see: Radin (2002a): 13.

¹⁸⁰⁹ GNU General Public License, Version 2, available at: <http://www.gnu.org/copyleft/gpl.html> (June 1991).

¹⁸¹⁰ Whether and to what extent loadable modules are in fact derivative works that are subject to § 2 of the GPL, is a difficult question that is beyond the scope of this article. No case law exists that directly addresses this question. As a general guideline, many commentators view modules that are statically linked to the kernel as derivative works, as opposed to dynamically linked modules. See: Jaeger, Metzger (2002): 43–45, 52–54; Asay (2002), 10–22; see also: E-mail from Linus Torvalds, available at: <http://www.atnf.csiro.au/people/rgooch/linux/docs/licensing.txt> (Oct. 19, 2001).

¹⁸¹¹ See: Behlendorf (1999): 167; see also: Radin (2002b): 1141.

¹⁸¹² However, this approach has some disadvantages as well. On the necessary tradeoff, see: Stallman (2002b). One alternative to the GPL that permits

Since September of 2001, the Linux system does not only rely on this legal allocation of rights, but also uses technology to enforce the desired openness of the system. In particular, the Linux kernel includes a mechanism that, before loading any module, checks whether the loadable module is GPL-compatible or not.¹⁸¹³ If the module's license terms do not allow its distribution under the GPL, the mechanism reports a warning and flags the kernel as "tainted".¹⁸¹⁴

While a detailed technical description of this mechanism is beyond the scope of this article,¹⁸¹⁵ it is important to realize that the Linux kernel uses technology to ensure that only software which adheres to the open source idea may use kernel functions. The Linux system uses a rudimentary rights expression language to express the license terms under which a module is distributed. The kernel reads this license string and either grants access, reports a warning or denies access to kernel components. This rights expression and enforcement mechanism is nothing less than a tiny DRM system.¹⁸¹⁶ The Linux kernel's DRM system is another example of how DRM technology may be used to preserve openness and protect a "commons" for creativity.¹⁸¹⁷

Symmetric Rights Expression Languages

DRM has also been severely criticized for overriding various limitations to copy-right law and for protecting content providers at the expense of legitimate interests of users and the public at large. Although this may be true for many current

the use of open source programs and libraries in proprietary programs is the "GNU Lesser General Public License" (LGPL), Version 2.1, available at: <http://www.fsf.org/copyleft/lesser.html> (Feb. 1999). For some information on the LGPL, see Nadan (2002): 360 note 51; Stallman (1999): 63; Jaeger, Metzger (2002): 50–54.

¹⁸¹³ For a general overview, see: Dankwardt (2002).

¹⁸¹⁴ Furthermore, the mechanism can also control that kernel symbols may only be used by modules which are licensed under the GPL; see: Dankwardt (2002); The Linux-Kernel Mailing List FAQ, at: <http://www.tux.org/lkml/#s1-19> (last updated Sept. 29, 2002).

¹⁸¹⁵ See: Dankwardt (2002); InsmoD Manpage, at: <http://lux.rm-rdf.com/man/man2html.cgi?insmod> (last updated Jan. 30, 2002).

¹⁸¹⁶ See also: posting of Alan Cox to linux-kernel@vger.kernel.org, at: <http://lwn.net/2001/0906/a/ac-tainted.php3> (Sept. 5, 2001). Preserving openness was not the only, or even the primary reason for including the described mechanism into the Linux kernel. Rather, some of the kernel developers became tired of receiving bug reports from users who are running proprietary modules in their systems; see: LWN.net, *Kernel Development*, at: <http://lwn.net/2001/0906/kernel.php3> (Sept. 6, 2001). Another example of a software system that uses DRM components to preserve openness is the "pragma License" in the Ada95 frontend to the GCC, GNAT; see: GNAT Reference Manual, at: http://gcc.gnu.org/onlinedocs/gcc-3.2/gnat_rm/Implementation-Defined-Pragmas.html.

¹⁸¹⁷ In addition, in April 2003, Linus Torvalds, the creator of the Linux kernel, opined that no legal or political reason exists why a more extensive DRM system could not be built into the Linux operating system, see: Posting of Linus Torvalds to the Linux Kernel Mailing List, at: <http://yro.slashdot.org/article.pl?sid=03/04/24/1312231> (Apr. 23, 2003).

commercial DRM implementations, it does not mean that the DRM concept is inherently hostile to fair use. Whether a DRM system respects fair use or not depends, in particular, on the design of the rights expression language. If fair use privileges and the other legitimate interests of information users cannot be expressed in the REL, such interests simply do not exist within the DRM system. Therefore, it is of utmost importance that RELs include semantics to express not only the interests of creators and rights holders (as all current RELs do), but also of information users (as no current REL does).¹⁸¹⁸

Recently, Deirdre Mulligan and Aaron Burstein have proposed changes to XrML that would create such a “symmetric” REL.¹⁸¹⁹ If, for example, the content provider uses metadata to prevent uses which fall under the fair use defense or other copyright limitations, a symmetric REL would offer the means to express the user’s request to engage in such use and communicate this to the DRM enforcement engine.¹⁸²⁰ Furthermore, a symmetric REL would include mechanisms to express the context in which DRM-protected content is used, so that the system may assess more accurately whether the user’s request is a fair use or not.¹⁸²¹ While expressing attributes such as locality and user intent in an REL might be a very complex issue, such expressiveness seems indispensable for creating a well-balanced REL. Mechanisms to distinguish between private and public uses would also be helpful, as copyright law often distinguishes along this line as well.¹⁸²² Symmetric RELs should be able to mark data that is not covered by copyright protection (such as mere facts under U.S. copyright law or works after their copyright term has ended).¹⁸²³

A symmetric REL could also involve various fair-use-friendly default settings. It could provide, for example, that users of a particular kind of work (such as electronic books) are always granted permission to use the work in certain ways (such as printing or private copying).¹⁸²⁴ Finally, it could include a default setting according to which pay-per-use models would not be employed and the tracking of individual usage patterns would be impermissible.¹⁸²⁵ Such approach might be even more promising in European *droit d’auteur* countries which, in contrast to the United States, limit their copyright protection not by a very broad and often fuzzy fair use doctrine, but by an enumerative list of discrete copyright limitations.¹⁸²⁶

¹⁸¹⁸ See: Mulligan, Burstein (2002): 4; Samuelson (2003): 42; Fox, LaMacchia (2003): 62–63.

¹⁸¹⁹ See: Mulligan, Burstein (2002); see also: Bechtold (2002): 48–49.

¹⁸²⁰ See: Mulligan, Burstein (2002): 7.

¹⁸²¹ See: Id.; see also: Felten (2003): 58.

¹⁸²² See: Mulligan, Burnstein (2002): 10.

¹⁸²³ See: Id.: 11–12.

¹⁸²⁴ See: Id.: 8–9; see also: Fox, LaMacchia (2003): 63.

¹⁸²⁵ See: Mulligan, Burnstein (2002): 9.

¹⁸²⁶ See also: Burk, Cohen (2001): 70; Felten (2003): 58; Fox, LaMacchia (2003): 63; Erickson (2003): 38.

While a symmetric REL is not a silver-bullet solution to reconcile DRM systems with copyright limitations, it would at least enable DRM systems to approximate the scope and importance of copyright limitations in general, thereby enabling consumers to use and access content without having to seek approval from rights holders.¹⁸²⁷ DRM systems that employ a symmetric REL would more closely align with the existing balance set by copyright law and could overcome much of the criticism related to fair use.¹⁸²⁸

Conclusion

In contrast to how it is sometimes described, DRM is not a synonym for absolute power of copyright owners over their creations. Rather, it provides an extremely flexible set of technologies that may be used for many different purposes. This is not to say that DRM will be able to cope with the whole range of copyright limitations and transformative uses in a manner of automated decision-making. It is just a critical remark about the current DRM discussions which do not take the full potential of DRM technology into account. Dynamic DRM systems may provide some tools to cope with cumulative innovation. DRM systems can also be used to preserve the commons in an open information environment. Finally, DRM systems may be built in which fair use privileges and other legitimate rights of information users can be managed and expressed. While current DRM implementations often fall short to fulfill such promises, this is just an indication that future DRM-related research and development should be focused on such issues. The potential of DRM for providing a balanced framework for the protection of both creators and users, i.e. a symmetric DRM, is far larger than usually acknowledged.

II.3 DRM Technology License Agreements and Fair Use

It has often been analyzed how DRM protects content by means of intertwining technology, anti-circumvention regulations, and usage contracts. However, it has been constantly overlooked that another means to protect digital content is DRM technology license agreements.¹⁸²⁹ This section will describe DRM technology license agreements and highlight their copyright implications.

¹⁸²⁷ But see: Felten (2003): 58–59, who argues that a DRM system trying to approximate the U.S. fair use doctrine is undesirable as such system would make too many errors leading to both undesired over- and underprotection of digital content. However, Felten's argument is much weaker in European *droit d'auteur* countries which do not have copyright limitations that are as vague as the U.S. fair use doctrine.

¹⁸²⁸ See also: Fox, LaMacchia (2003): 62–63 (aptly pointing out that the creation of a symmetric REL is only one step towards a fair-use-protecting DRM system). For a different approach to reconcile DRM with copyright limitations for private copying, see: Neubauer, Brandenburg, Siebenhaar (2002) (proposing a “light weight” DRM system that would allow users to transfer content to portable devices and transmit it to friends while discouraging them from engaging in mass-scale piracy).

¹⁸²⁹ So far, the relationship between DRM technology licenses, antitrust and copyright policy has only been analyzed thoroughly by Weinberg (2002) for a specific

Many DRM technologies are protected by a patent or kept as a trade secret. If a computer or consumer electronics manufacturer wants to enable his devices to process content that is protected by such DRM technology, it has to enter into a technology license agreement with the developer of the technology.¹⁸³⁰ Licensees of DRM technologies include manufacturers of consumer electronics, computers, storage media and other DRM-enabled devices or components as well as content providers. Licensors of DRM technologies are either the companies which have developed the DRM technology or specialized licensing authorities that administer the licensing process on behalf of these companies.¹⁸³¹

Although content providers are usually not licensors of DRM technology, due to a rather complex mix of interests, DRM technology license agreements indirectly serve their interests.¹⁸³² This explains why various license agreements include copyright-related terms.¹⁸³³ DRM technology licenses attempt to prevent unauthorized copying. Various licenses restrict the quality or speed by which content is transmitted, making piracy less attractive as it either takes too long or leads to inferior copies.¹⁸³⁴ They also require that DRM-enabled devices obey the

license in the pay TV sector (“POD-Host Interface License Agreement”) and by Bechtold (2002): 178–196, 405–406, for such licenses in general; see also: Marks, Turnbull (2000): 206.

¹⁸³⁰ Apart from Sony, there are no major content companies that also produce consumer electronics or vice versa.

¹⁸³¹ Such licensing authorities include the DVD Copy Control Association, Inc. (<http://www.dvcca.org>), the Digital Transmission Licensing Administrator (<http://www.dtcp.com>), the 4C Entity, LLC (<http://www.4centity.com>), and Digital Content Protection, LLC (<http://www.digital-cp.com>).

¹⁸³² The short version of the story is that content providers will only release content in a DRM system if certain security requirements are met. Therefore, content providers are in the position to force DRM technology companies to alter their technology and the related license agreements according to the content providers’ interests; for more information, see: Bechtold (2002): 180; Weinberg (2002): 286; *In re Implementation of Section 304 of Telecommunications Act of 1996*, 15 F.C.C.R. 18199, Par. 15, 27 (Sep. 18, 2000); see also: Marks, Turnbull (2000): 206.

¹⁸³³ For the following analysis, most of the publicly available DRM technology licenses were evaluated. The evaluated licenses include the CSS, CPRM/CPPM, DTCP and HDCP license agreements. For more information on the underlying technologies, see *infra* notes 1936–1939. In addition, the POD-Host Interface License Agreement (“PHILA”) was evaluated. This license deals with a decryption technology (“Dynamic Feedback Arrangement Scrambling Technique”, DFAST) that is used in U.S. pay TV decoders. For more information, see: Weinberg (2002): 287–288; Bechtold (2002): 184; *In re Implementation of Section 304 of Telecommunications Act of 1996*, Commercial Availability of Navigation Devices, 15 F.C.C. Rcd. 18199 (F.C.C. 2000). DFAST is also licensed under other licensing terms, see: *Consensus Cable MSO — Consumer Electronics Industry Agreement on “Plug & Play” Cable Compatibility and Related Issues*, available at: http://www.ncta.com/pdf_files/CE-NCTAagreement.pdf (Dec. 19, 2002).

¹⁸³⁴ See: § 2.3, Exhibit C, POD-Host Interface License Agreement, available at: http://www.opencable.com/downloads/PHILA_101702.pdf (Oct. 17, 2002); §§ 4.2.1 (ii), (iii), 5.1, 5.2.2, Exhibit C-1, and §§ 4.2.1 (ii), (iii), 6.1.2, Exhibit C-2, CPRM/CPPM License Agreement, Version 1.1f, available from: http://www.4centity.com/licensing/adopter/adopter_form.html.

usage rules of digital content that are defined by the content provider. If, for example, the content provider has embedded a digital watermark into his content prescribing that the content may only be copied once, all consumer devices that use the licensed DRM technology are contractually required to ensure through technology that a user can indeed make only one copy.¹⁸³⁵

Although DRM technology license agreements raise many more questions,¹⁸³⁶ for the purposes of this article, it is sufficient to note that they may come into conflict with copyright law. DRM technology licenses enable content providers to make sure that all consumer devices that can access their DRM-protected content adhere to certain usage rules. Although they do not directly supersede copyright limitations, they can prevent device manufacturers from producing devices that would enable consumers to benefit from copyright limitations, as this would constitute a breach of the technology license.¹⁸³⁷ Thereby, DRM technology license agreements may contribute indirectly to the *de facto* undermining of copyright limitations.

The potential tension between DRM technology license agreements and copyright limitations has been very rarely addressed by legislatures or the administration. In Europe, the matter has not been tackled at all.¹⁸³⁸ In the United States, in its assessment of a DRM technology license in the pay TV sector,¹⁸³⁹ the Federal Communications Commission (FCC) rejected the claim that the license would preclude reasonable home recording of DRM-protected content.¹⁸⁴⁰ Although the FCC did not take action against the DRM technology license, this instance shows a possible method of reconciling technology licenses with copy-

¹⁸³⁵ See: § 2, Exhibit B, Part 1, Digital Transmission Protection License Agreement, at: http://www.dtcp.com/data/DTCP_Adopters_Agreement010730.PDF (July 30, 2001); § 3, Exhibit C, POD-Host Interface License Agreement, *supra* note 1834; §§ 4.1.4, 4.2.1 (i), Exhibit C-1, §§ 3.1.1 a), 3.2.2, § 4.2.1 (i), Exhibit C-2, §§ 3.1.1, 3.1.2, 4.2.1 (i), 4.2.2. (i) Exhibit C-3, CPRM/CPPM License Agreement, *supra* note 1834.

¹⁸³⁶ See: Bechtold (2003a); Bechtold (2002): 178–196, 377, 405–406.

¹⁸³⁷ See: Weinberg (2002): 292.

¹⁸³⁸ However, the possible tension between DRM technology licenses and other areas of public policy, in particular antitrust law, have long been recognized in Europe, see *infra* text accompanying notes 1891–1892.

¹⁸³⁹ For information on the “POD-Host Interface License Agreement”, see *supra* note 1833.

¹⁸⁴⁰ *In re Implementation of Section 304 of Telecommunications Act of 1996*, *supra* note 1833, at Par. 28–29. That the FCC recognized the possible tension between DRM technology licenses and copyright limitations becomes evident in the separate statement of Commissioner Gloria Tristani: “[...] *our ruling in no way authorizes any attempt by providers of services to utilize this ruling to combine technology with copy protection in a manner that interferes with, or unreasonably restricts, a consumer’s fair use of copy-protected material. [...] Today’s declaration ensures the financial rewards of copy protection to content owners while protecting citizens from the dispossession of their right to fair use. Based on the record before us and controlling Supreme Court precedent, I believe we have struck the appropriate balance*”, Id. at 18220. See also: Weinberg (2002): 289–292 (criticizing the FCC’s failure to recognize the underlying public policy concerns).

right limitations: limiting the range of terms licensors can write into a DRM technology license.¹⁸⁴¹

II.4 DRM and Research

DRM-related anti-circumvention regulations may create chilling effects on scientific research and progress. In 2000, Princeton University Professor Edward Felten and several coauthors intended to present a research paper at a scientific conference that described weaknesses in several watermarking systems which the “Secure Digital Music Initiative” (SDMI) was considering to adopt at that time. The Recording Industry Association of America (RIAA) and SDMI threatened Professor Felten and his coauthors with a lawsuit because, as they claimed, the publication of the paper would violate the anti-circumvention provisions of the Digital Millennium Copyright Act (DMCA). As a result, the authors decided to withdraw the paper from the conference.¹⁸⁴² In other instances, concerns about potential circumvention liabilities prompted researchers to withhold the results of their research or even not to engage in DRM-related security research at all.¹⁸⁴³

To understand the potential tension between anti-circumvention provisions and security research, it is important to realize how security research works. Practical experiments and tests are indispensable for evaluating the features and security level of any real-world implementation of a security system. One of the standard approaches to evaluate a real-world security system is to attempt to break it. If a researcher succeeds in breaking it, he publishes his procedure and results, thereby enabling other members of the security research community to understand his attack and build more secure systems.¹⁸⁴⁴ By impeding such security research, the legal framework surrounding DRM could have detrimental impact on technological innovation in the area of security systems.

At least to some extent, the legislators on both sides of the Atlantic were aware of this tension between anti-circumvention regulations and scientific research. Yet, they may not have done enough to resolve it. The U.S. DMCA exempts certain acts of security testing, reverse engineering, and cryptography research from the anti-circumvention provisions. However, these exemptions are narrowly drawn and cover only a small subset of legitimate security research.¹⁸⁴⁵ In the European

¹⁸⁴¹ See: Bechtold (2002): 405–406. This is not a totally novel approach, as the limitations on DRM technology licenses due to antitrust concerns demonstrate, see *infra* text accompanying notes 1891–1892.

¹⁸⁴² The authors then sought a judicial declaration that their paper did not violate the DMCA. Later, this complaint was dismissed because SDMI and RIAA had withdrawn their objections to the publication of the paper; see: Samuelson (2001); Samuelson, Scotchmer (2002): 1647 note 333; Harper (2002); Imfeld (2003): 138.

¹⁸⁴³ See: Electronic Frontier Foundation (2003): 2–5; see also: Liu (2003).

¹⁸⁴⁴ See: Committee on Intellectual Property Rights and the Emerging Information Infrastructure (2000): 313–318; see also: Preston, Lofton (2002): 85–95.

¹⁸⁴⁵ See: Samuelson (2001): 2029; Samuelson (1999): 548–549; Committee on Intellectual Property Rights and the Emerging Information Infrastructure (2000): 318–321; see also: Preston, Lofton (2002): 119–125; Liu (2003).

Copyright Directive, the tension between anti-circumvention regulations and security research is only mentioned in a Recital.¹⁸⁴⁶

Nevertheless, one should be cautious about condemning DRM and anti-circumvention regulations on these grounds. Whether anti-circumvention regulations actually impede security research depends on many factors related to the individual technology that was tested, the way the testing was done and publicized, the persons involved, the wording of the particular anti-circumvention regulation that is applied and so on.¹⁸⁴⁷ In some cases where an impediment of security research is claimed, such claims turn out to be unfounded.

Furthermore, the tension between anti-circumvention regulations and security research is not only a problem of the law, but also of technical security design. The more a security architecture adheres to the so-called Kerckhoff principle, the less strong this tension is.¹⁸⁴⁸ Unfortunately, this does not fully resolve the tension between anti-circumvention regulations and scientific research. There are many areas of computer security where the Kerckhoff principle does not apply, and quite often real-world implementations do not adhere to the Kerckhoff principle due to financial or technical constraints. As a result, security in most current DRM implementations does not adhere to the Kerckhoff principle, but is rather achieved by obscurity approaches, for example by using various code obfuscation technologies.¹⁸⁴⁹ Nevertheless, this demonstrates that striving for compliance with the Kerckhoff principle is not only a matter of good security systems design, but would also alleviate the tension between anti-circumvention regulations and security research.

In general, however, it is a troublesome development that various species in the ever-expanding world of intellectual property, including anti-circumvention regulations, increasingly come into conflict with the freedom of scientific research and thereby technological progress.¹⁸⁵⁰

¹⁸⁴⁶ Recital 48 of the Directive 2001/29/EC of the European Parliament and of the Council of May 22, 2001, on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society, Official Journal of the European Communities L 167 (June 22, 2001), 10, 14 (hereinafter: European Copyright Directive) (stating that circumvention prohibitions “should not hinder research into cryptography”).

¹⁸⁴⁷ For an in-depth analysis of the DMCA’s impact on encryption research, see: Liu (2003).

¹⁸⁴⁸ The Kerckhoff principle is widely accepted in cryptology research. It states that the security of an encryption system should not be based on the secrecy of the algorithm used, but only of particular keys employed. One of the consequences of the Kerckhoff principle is that unaffiliated security researchers may openly discuss the security features of the (publicly known) encryption algorithm without revealing any secrets. For more information on the Kerckhoff principle, see: Schneier (1996): 5; Anderson (2001): 240, 362; see also: State of New York v. Microsoft Corp., 224 F.Supp.2d 76, 238–239 (D.D.C. Nov. 1, 2002).

¹⁸⁴⁹ See: Bechtold (2002): 88–89. For more information on code obfuscation, see *infra* notes 1884–1885.

¹⁸⁵⁰ In the biotechnology area, concerns have been raised over the last few years that by issuing patents for biotechnological research tools and covering them with

III DRM, Property and Liability Rules

For several decades, copyright law has been grappling with the question of how to deal with private copying by consumers. With the emergence of cassette recorders and photocopying machines, it became evident that private copying was a mass-scale phenomenon that was very hard to control. For this and other reasons, many European legislators created a copyright exemption for private copying, but compensated rights holders indirectly by creating a levy system which imposes a levy on all blank media and copying devices being sold.¹⁸⁵¹

Today, 12 of the 15 member states of the European Union have put in place levy systems of different flavors.¹⁸⁵² In Germany, which was the first country to create a statutory levy system in 1965, some of the levies are:¹⁸⁵³

audio recording devices (except MP3 players)	€1,28	per device
audio recording media	€0,0614	per hour
MP3 players	€2,56	per player
video recording devices	€9,21	per device
video recording media	€0,087	per hour
CD burners	€6,50 – 7,00	per burner

These levies are collected by collecting societies which distribute the revenues (about 71 million € in 2000) among their members. In the United States, only the Audio Home Recording Act of 1992 includes a levy system for digital audio recording devices and blank storage media. There, the levy amounts to 2 or 3% of the price of the device or media.¹⁸⁵⁴ However, the Audio Home Recording

so-called “reach-through licenses”, biological research that depends on these tools could be impeded; see: Goldstein (2001); Eisenberg (2001); see also: Ware (2002); Mueller (2001); Heller, Eisenberg (1998).

¹⁸⁵¹ In Germany, compensating rights holders for the private copying exemption was one of the main reasons for introducing the levy system in 1965; see: Loewenheim in: Schricker (1999): § 53 notes 1–2, § 54 note 2. For a history of the levy system in European countries, see: Hugenholtz, Guibault, van Geffen (2003): 10–13.

¹⁸⁵² See: Hugenholtz, Guibault, van Geffen (2003): 12 (listing Germany (1965), Austria (1980), Finland (1984), France (1985), Netherlands (1990), Spain (1992), Denmark (1992), Italy (1992), Belgium (1994), Greece (1994), Portugal (1998), and Sweden (1999)). Worldwide, at least 42 countries have a remuneration scheme for private copying, see: Id. 13.

¹⁸⁵³ See: § 54 of the German Copyright Act; see also: Kreile (1992). In addition, in February 2003, the arbitration board of the German Patent and Trademark Office (Deutsches Patent- und Markenamt) ruled that, for every PC sold in Germany, a levy of €12 should be paid, see: <http://www.giantstepsmts.com/DRM%20Watch/germanpclevy.htm>; Hugenholtz, Guibault, van Geffen (2003): 26. The PC manufacturing industry has strongly objected to the settlement proposal. It is expected that, ultimately, courts will have to decide whether PCs are subject to a levy under German copyright law or not. For some valid criticism of attempts to extend levy schemes to computers, see: Hugenholtz, Guibault, van Geffen (2003): 40–41.

¹⁸⁵⁴ 17 U.S.C. §§ 1003, 1004.

Act has a narrow scope. In particular, MP3 players are not covered by its levy system.¹⁸⁵⁵

Levy systems curtail the rights of copyright and neighboring rights holders. With copyright, rights holders cannot only ensure to receive *remuneration* for the use of their works, but they can also *control* who uses their content in which ways and under what circumstances. In a levy system, rights holders lose this power to control, but retain the power to receive remuneration. In law-and-economic terms, levy systems turn copyright from a property rule to a liability rule.¹⁸⁵⁶ In this regard, levy systems are similar to compulsory licensing schemes: both approaches deprive rights holders of their ability to control who uses their content under what circumstances. What they are left with is the ability to receive remuneration for the use of their content.

With DRM systems, controlling private copying becomes technically feasible. This raises the question whether and to what extent existing levy systems can be justified in a DRM-suffused environment. On both sides of the Atlantic, the relationship between DRM and levy systems or related approaches is heavily discussed, albeit with sometimes opposing results.

In Europe, many DRM proponents argue that levy systems should be abandoned in favor of DRM systems. Both systems, they argue, cannot coexist: if a levy is imposed indirectly on consumers while, at the same time, they are required by DRM systems to pay for each private copy they make, consumers would end up being charged twice.¹⁸⁵⁷ Furthermore, DRM enables a more direct remuneration of the rights holders whose works are actually consumed. Compared to a levy system, DRM is, so the argument goes, more just, more precise and more efficient.¹⁸⁵⁸ According to this argument, levy systems should be abandoned, while DRM systems should be supported.¹⁸⁵⁹ This argument is supported by the European Copyright Directive of 2001 which seems to favor a gradual phasing-out of levies on digital media or equipment in favor of DRM systems.¹⁸⁶⁰

¹⁸⁵⁵ See: Recording Industry Ass'n of America v. Diamond Multimedia Systems, Inc., 180 F.3d 1072 (9th Cir. 1999).

¹⁸⁵⁶ See: Calabresi, Melamed (1972).

¹⁸⁵⁷ See: Hugenholtz, Guibault, van Geffen (2003): 34.

¹⁸⁵⁸ See: Huppertz (2002): 108; Hart (2002): 60; Walker, Sharpe (2002): 260–261; see also: Hugenholtz, Guibault, van Geffen (2003): 32–47. This argument also raises the question what role collecting societies, which — among many other things — administer many levy systems, can still play in a DRM-suffused environment; see: Bechtold (2002): 11–13; see also: Jehoram (2001); Merges (1996); Kretschmer (2002); Hugenholtz, Guibault, van Geffen (2003): 47. See further: Günnewig (page 528); Ulmer–Eilfort (page 447) within this book.

¹⁸⁵⁹ An alternative solution would be to enact a broad levy system, but to disregard such content providers in the levy distribution process which use DRM systems to protect their content. The amount of the levy would create an upper bound up to which DRM technology companies could license their technologies to device manufacturers (as it would be cheaper for device manufacturers to use the levy system for content protection if the DRM technology license fee would be more expensive than the device levy).

By contrast, U.S. scholars have proposed to expand the liability rule regime considerably while condemning the DRM regime.¹⁸⁶¹ While adequate remuneration for creators is an essential incentive for creativity, any über-protection of creators may harm innovation in regards to distribution technology and content itself. Empowering creators to control who uses their content under what circumstances, the argument goes, may be such an über-protection. Therefore, it may be a wise policy and economic decision to cut the power of rights holders back to a mere right to become remunerated — a compulsory licensing scheme or a levy system.¹⁸⁶² The goal is, as Lawrence Lessig puts it, “compensation without control”.¹⁸⁶³

It is interesting to note that in Europe and the United States, opposite DRM policy proposals are articulated and discussed. In Europe, a move from the generalizing levy system to more individualized DRM solutions can be observed, while in the United States, academic circles argue to move from DRM to a levy system.

Although it is probably true that a regulatory system of perfect control would be a bad policy choice for intellectual property law, it is beyond the scope of this article to answer the question of what the optimal policy decision along the alleged axis between a levy or a compulsory licensing scheme and DRM

¹⁸⁶⁰ See: Article 5 (2) (b) of the European Copyright Directive, *supra* note 1846, at 10 (stating that member states may provide for limitations to the reproduction right “[...] *in respect of reproductions on any medium made by a natural person for private use and for ends that are neither directly nor indirectly commercial, on condition that the rightholders receive fair compensation which takes account of the application or non-application of technological measures [...]*”) and Recital 39 of the Directive (stating that in regards to the private copying limitation, member states “[...] *should take due account of technological and economic developments, in particular with respect to digital private copying and remuneration schemes, when effective technological protection measures are available*”); see also: Recital 35. In Germany, Article 5 (2) (b) of the Copyright Directive is likely to be implemented as a new subparagraph of § 13 of the Urheberrechtswahrnehmungsgesetz, see Artikel 2 des Entwurfs eines Gesetzes zur Regelung des Urheberrechts in der Informationsgesellschaft, Bundestags-Drucksache 15/837 vom 9. 4. 2003, S. 1, 22. For a comprehensive analysis of the relationship between DRM and levies under the European Copyright Directive, see: Hugenholtz, Guibault, van Geffen (2003).

¹⁸⁶¹ See, e.g.: Netanel (2003) (proposing a statutory levy system for P2P software and services, computer hardware, CD burners, MP3 players, digital video recorders, and blank media while precluding content providers from employing DRM systems to block activities that are covered by the levy system); Sobel (2003) (proposing to impose a statutory license on the copying and redistribution of digital content, to embed digital watermarks and fingerprints into the content so that Internet service providers can monitor the content flow through their servers, and to obligate ISPs to pay a royalty charged by each work’s copyright owner); Lunney (2001): 911–918. William Fisher makes a similar argument in chapter 6 of his forthcoming book “Promises to Keep — Technology, Law, and the Future of Entertainment”. See also: Lessig (2001): 254–255.

¹⁸⁶² See: Lessig (2001): 107–110, 199–202, 216–217, 254–255.

¹⁸⁶³ See: *Id.*: 201.

is. Rather, this subsection attempts to show that, in fact, no such axis exists. DRM is not the same as perfect control. Or, at least, it does not have to be. DRM is also not the opposite of a levy system, a compulsory licensing scheme or a liability rule. Properly understood, DRM technology is much more flexible than most of its critics acknowledge. Besides control technologies such as access control and encryption, DRM includes technologies to manage content flows, to describe content, users and devices, as well as to describe and prove the authenticity and integrity of content, users, metadata and devices.¹⁸⁶⁴ It is possible to design a DRM system that does not grant utmost control to rights holders, but only enables them to receive adequate remuneration.¹⁸⁶⁵ Indeed, even levy and compulsory licensing systems could be based on DRM technology.¹⁸⁶⁶

Therefore, to ask whether a levy system or a DRM solution should be preferred is to ask the wrong question. Rather, it should be asked whether a copyright regime that is solely based on a property rule approach is preferable over a regime that includes well-placed elements which are based on a liability rule approach. The discussion along the alleged DRM — levy axis does not answer this question. Only after this question has been answered can one think about the appropriate technologies that should be used to achieve the desired incentive structure.

IV DRM and Privacy

While it is still unclear what role DRM should and will play in the intellectual property system, its relation to other areas of law is fuzzy as well. This applies particularly to privacy law. DRM systems use various mechanisms to identify and track users within the system. They have the potential to monitor what people privately read, listen to or watch.¹⁸⁶⁷ On the other hand, such usage information may be useful both to content providers and consumers: content providers can engage in price discrimination, which may lead to lower prices for some consumers.¹⁸⁶⁸ All consumers could also benefit from a better personalization and individualization of the service.

¹⁸⁶⁴ See *supra* note 1785.

¹⁸⁶⁵ Digital watermarks could be used to describe digital content, tamper-resistant hard- and software could be used to meter usage of the content which would be the basis for payment flows to the rights holders. Although such system would still manage rights in a digital way, no component would restrict access to any content. Rather, anybody would be free to use content as long as he would be willing to pay for it. In this sense, such a DRM system would distribute content as “free resources” as defined by Lessig (2001): 12, 20.

¹⁸⁶⁶ See: Netanel (2003): 38–39 (proposing to distribute the proceeds of suggested levy system to rights holders in proportion to the usage of their respective works, as measured by DRM technology); Sobel (2003): 12–13 (suggesting to use digital watermarks and fingerprints to support his proposed statutory licensing regime); Hugenholtz, Guibault, van Geffen (2003): 45 (proposing to embed metadata in recording equipment and media to indicate to a DRM system that a levy has been paid).

¹⁸⁶⁷ See: Bygrave, Koelman (2000); Cohen (1996); Bygrave (2002a); Bizer (2001).

In this muddy mixture of privacy, competition, consumer protection and business interests, a clear regulatory approach as to how to reconcile DRM with privacy laws does not exist yet.¹⁸⁶⁹ What is particularly unfortunate is that there is a clear lack of discussion about what role privacy-enhancing technologies (PETs) can and should play in DRM systems.¹⁸⁷⁰ Furthermore, it should be reminded that the acronym DRM does not stand for “digital copyright management”, but for the management of *rights in general*.¹⁸⁷¹ It is interesting to analyze how DRM systems can be adapted in order to manage and protect privacy rights.¹⁸⁷²

The design of a DRM system shapes its privacy implications. This becomes particularly obvious with the design of metadata systems. It is an open question as to what the optimal granularity is with which digital objects should be identified by a metadata system. Should a text be only identifiable in its entirety or should each paragraph, sentence, word or even character be identifiable by the metadata system?¹⁸⁷³ While there are many technical and efficiency reasons for preferring one approach over the other, it is important to realize that the

¹⁸⁶⁸ In general, price discrimination becomes particularly attractive if the fixed costs are high and the marginal costs are low. This applies, e.g., to digital content. DRM systems offer technologies that can clear two of the most important hurdles to price discrimination: identifying different users with different preferences and preventing arbitrage between such users; see: Bechtold (2002): 307–311. Whether price discrimination is beneficial from an economic perspective and should therefore be used in real-world DRM systems is a hard question; for some valid criticism against this conclusion, see: Boyle (2000); Cohen (2000): 1801–1806; Gordon (1998): 1381, 1386–1389; Bechtold (2002): 321–324.

¹⁸⁶⁹ While both the European Copyright Directive and the U.S. DMCA address the tension between DRM systems and privacy laws, they do not offer such an approach; see: Bygrave (2002a): 54–56; Bygrave, Koelman (2000): 106–120; Samuelson (1999): 552–554.

¹⁸⁷⁰ For an overview of the role PETs could play in DRM systems, see: Bechtold (2002): 138–142. For another, rather different and critical proposal, see: Feigenbaum, Freedman, Sander, Shostack (2001).

¹⁸⁷¹ This insight was best expressed by Victor Shear, then CEO of InterTrust, in a Congressional hearing: “*Ultimately, the reality of sophisticated DRM technology is about far more than Napster, online entertainment and copyright law. It is about constructing a civil digital society in the Internet Age, where rules created for or by its citizens can be implemented and respected wherever and whenever their legitimate interests are in play*”, Testimony Before the U.S. Senate Judiciary Committee on Online Entertainment and Copyright Law, Apr. 3, 2001, 2001 Westlaw 323735. Indeed, as DRM reveals, strong similarities between copyright and privacy exist in the digital age. In both cases, the law tries to allocate rights to individuals in order to solve conflicts of interests. In both cases, the subject of these rights is information in various forms.

¹⁸⁷² See: Kenny, Korba (2002); Zittrain (2000).

¹⁸⁷³ See: Paskin (1999); Kroon (2000): 231; Bechtold (2002): 39. A related problem is whether information about the content should be embedded in the content itself or should be stored in a separate database. In the area of metadata systems, this led to a long-lasting battle between “intelligent” and “dumb” identifiers. Choosing an appropriate architecture along these lines has not only efficiency, but also privacy implications; see: Paskin (1999): 1209, 1213–1214; Paskin within this book on page 26; Hill (1999): 1232; Bechtold (2002): 38.

design of the metadata system has privacy implications as well. The more precisely an object can be identified, the better and more extensive usage data can be collected and processed. Determining the granularity of a metadata system determines its implications for privacy interests as well. Furthermore, rights expression languages could be designed to minimize expressions of personally identifying information.¹⁸⁷⁴ Consumers could be given control over the entities that process their data and consumption requests.¹⁸⁷⁵

Although this article does not attempt to provide specific guidelines of how to implement a privacy-protecting DRM system, it attempts to show that the discussion about such issues could actually lead to a DRM design that truly respects and protects the various legitimate privacy interests of its users.¹⁸⁷⁶

V DRM and Competition

Increasingly, DRM systems are used to protect hardware and software platforms.¹⁸⁷⁷ Such protection may harm competition, either in the platform market itself or in complementary markets. In analyzing these developments, issues such as antitrust, innovation, and security concerns as well as the free movement of goods have to be taken into account. As this section will demonstrate, anti-circumvention regulations are increasingly used in circumstances for which they were clearly not intended. Increasingly, DRM technologies and anti-circumvention regulations are not only used to control content against unauthorized copying, but also to control markets against undesired competition.

V.1 Competition in the Platform Market

More and more, manufacturers of hardware and software platforms use DRM components to prevent competitors from developing and marketing competing platforms. In particular, DRM technologies and anti-circumvention regulations are used to create proprietary interfaces to the platform, thereby foreclosing entry into the platform market.¹⁸⁷⁸ Three examples, from computer games and pay TV decoders to patented DRM components, may illustrate this point.

¹⁸⁷⁴ This could mean to limit the expressive functionality of rights expression languages so that they could not be used to express and gather personally identifying information; see: Mulligan, Burstein (2002): 12–13.

¹⁸⁷⁵ See: *Id.*: 13.

¹⁸⁷⁶ For interesting proposals to reconcile DRM with privacy interests on these grounds, see: Cohen (2003).

¹⁸⁷⁷ A technology platform is a good that a consumer can acquire to make use of complementary goods that depend on the platform. Desktop computers, video game consoles and operating systems are examples of such platforms. For an overview of the legal problems of such platforms, see: Lichtman (2000); Weiser (2002); Weiser (2001a); Weiser (2001b); Houweling (2002); Samuelson, Scotchmer (2002): 1611, 1615–1626.

¹⁸⁷⁸ See: Samuelson, Scotchmer (2002): 1645.

Reverse Engineering DRM-Protected Platforms

Developers of hard- or software platforms (such as personal computers, video game consoles or operating systems) have strong interests in preventing competitors from developing interoperable platforms, as this could reduce the developers' market share. By contrast, competitors have strong interests in being able to reverse engineer the dominant technology platform in order to develop a competing and interoperable platform. Whether and to what extent reverse engineering should be allowed and how this alters incentive structures for software developers is a question that has received considerable attention in the scholarly debate.¹⁸⁷⁹ As this subsection will show, protecting technology platforms with DRM components may alter the balance between copyright protection and reverse engineering limitations, which are enshrined in many countries' copyright laws. If a technology platform is protected by a DRM system, reverse engineering may not only violate traditional copyright law, but also anti-circumvention regulations. Thereby, the relationship between anti-circumvention regulations and reverse engineering activities becomes essential.

Two examples may illustrate this point. Blizzard Entertainment¹⁸⁸⁰ markets several highly successful computer games which can be played over the Internet in a multi-player mode. In order to play a Blizzard game in such a mode, each user has to connect to an Internet gaming server operated by Blizzard. Since 1998, a small software company has been analyzing the internal operation of Blizzard's gaming network in order to develop a software program called "bnetd" which emulates Blizzard's gaming server. With bnetd, users can form online gaming communities and play Blizzard's games without having to use Blizzard's online server. In the spring of 2002, Blizzard filed a lawsuit against the bnetd developers. Among other things, Blizzard claims that its gaming network is protected by various technological measures, and that the development of a competing gaming server is an infringement of the DMCA's anti-circumvention provisions. By contrast, the bnetd developers view their activity as lawful reverse engineering that is aimed at creating an interoperable, competing gaming server.¹⁸⁸¹

Another example of the tension between DRM-protected platforms and reverse engineering activities is the Sony Playstation. In 1999 and 2000, Sony filed two copyright- and patent-based lawsuits against two companies that had developed software programs which emulated Sony's video game console "Playstation". By using one of these programs, the user could play Playstation games on his personal computer without having to buy a Sony game console at all.¹⁸⁸² These

¹⁸⁷⁹ See only: Samuelson, Scotchmer (2002).

¹⁸⁸⁰ Blizzard Entertainment is a division of Vivendi Universal Games, Inc.

¹⁸⁸¹ For more information on the case, see: the EFF's Blizzard v. bnetd archive page, at: http://www.eff.org/IP/Emulation/Blizzard_v_bnetd (last updated Mar. 13, 2003); Miller (2002).

¹⁸⁸² Sony Computer Entm't, Inc. v. Connectix Corp., 203 F.3d 596 (9th Cir. 2000); Sony Computer Entm't Am., Inc. v. Bleem, LLC, 214 F.3d 1002 (9th Cir. 2000); see also: Karas (2001): 48; Samuelson, Scotchmer (2002): 1611.

emulations were made possible by reverse engineering various technical components of Sony's Playstation.¹⁸⁸³

Even if anti-circumvention regulations include an exemption for reverse engineering activities, this may still not enable competitors to develop a competing platform. Various DRM technologies exist — including “code obfuscation” technologies and similar approaches to create tamper-resistant software¹⁸⁸⁴ — which render attempts to reverse engineer either very costly or even impossible.¹⁸⁸⁵ Even if the law allows reverse engineering, this can remain a hollow promise in a DRM-protected technology platform if reverse engineering is simply impossible due to technical or financial reasons.¹⁸⁸⁶ Using DRM to protect technology platforms may therefore impede competition in the platform market.

Patenting DRM Components

Another example of how competition in the DRM platform market may be impeded involves patents on DRM components. In December 2001, Microsoft obtained approval for two U.S. patents that contain many of the basic elements of a DRM-enabled operating system.¹⁸⁸⁷ DRM veteran company Intertrust has been issued 26 U.S. DRM-related patents up to date.¹⁸⁸⁸ At the very least, patents on DRM components raise the general question of whether and to what extent standards should be subject to intellectual property rights.¹⁸⁸⁹ Like every patent on technology standards, DRM patents can also be used strategically. In the context of Microsoft's Palladium initiative, for example, critics have warned that Microsoft could use its patents over the Palladium design to thwart attempts of open source programmers to create a Linux version that could be executed on Palladium-enabled PC hardware.¹⁸⁹⁰

¹⁸⁸³ See, e.g.: Sony v. Connectix, 203 F.3d 596, 599–601 (9th Cir. 2000). It is noteworthy that in both of these cases, the use of DRM components to protect the technology platform was not an issue before the court.

¹⁸⁸⁴ For an overview, see: Goto (2001): 145–146; see also: Bechtold (2002): 87–89.

¹⁸⁸⁵ Of course, this presupposes that technologies such as code obfuscation are effective means to protect against reverse engineering. For a theoretical rebuttal of the idea of code obfuscation, see: Barak et al. (2001).

¹⁸⁸⁶ For some policy proposals to address this problem, see: Samuelson, Scotchmer (2002): 1661–1662.

¹⁸⁸⁷ *Digital Rights Management Operating System*, U.S. Patent 6,330,670 (issued Dec. 11, 2001); *Loading and Identifying a Digital Rights Management Operating System*, U.S. Patent 6,327,652 (issued Dec. 4, 2001).

¹⁸⁸⁸ Since April 2001, a lawsuit is pending between Intertrust and Microsoft in which the validity, scope and ownership of various DRM-related patents is analyzed.

¹⁸⁸⁹ See, e.g.: Lemley (2002).

¹⁸⁹⁰ Indeed, in its Palladium FAQ, even Microsoft addresses this concern and gives the succinct answer: “*It is too early to speculate on how those issues might be addressed*”, see: Microsoft Corp. (2003). For more information on Palladium, see *infra* text accompanying notes 1986–1999.

DRM Technology License Agreements and Competition

Finally, DRM technology license agreements may be used in anti-competitive ways as well. In the area of pay TV, European legislation has tried to deal with the potential tension between DRM technologies protected by intellectual property rights and a well-functioning competition. Standards developed by the “Digital Video Broadcasting Project” (DVB) allow several competing DRM systems (so-called “conditional access systems”, CAS) to be included in one single Pay TV decoder.¹⁸⁹¹ This architecture and related approaches enable competition to occur between different providers of DRM systems in the pay TV market. In order to protect this competition, the recently adopted European Access Directive prohibits DRM technology providers from using technology license agreements to thwart this competition, either by preventing interoperability between different DRM systems or by preventing the inclusion of a competing DRM system in the same decoder.¹⁸⁹² This regulatory approach prevents DRM technology providers from using license agreements to impede competition in the DRM-protected platform market.

¹⁸⁹¹ Describing the underlying technologies is beyond the scope of this article. For more information on SimulCrypt, MultiCrypt, the Common Interface, as well as Entitlement Management Messages (EMM) and Entitlement Control Messages (ECM), see: Bechtold (2002): 105 note 522; Llorens-Maluquer (1998): 560–563; European Commission (1999).

¹⁸⁹² See Annex I, Part I, lit. (c) to Article 6 (1) of the Directive 2002/19/EC of the European Parliament and of the Council of March 7, 2002, on Access to, and Interconnection of, Electronic Communications Networks and Associated Facilities (Access Directive), Official Journal of the European Communities L 108 (Apr. 24, 2002), 7:

“when granting licences to manufacturers of consumer equipment, holders of industrial property rights to conditional access products and systems are to ensure that this is done on fair, reasonable and non-discriminatory terms. Taking into account technical and commercial factors, holders of rights are not to subject the granting of licences to conditions prohibiting, deterring or discouraging the inclusion in the same product of:

- *a common interface allowing connection with several other access systems, or*
- *means specific to another access system, provided that the licensee complies with the relevant and reasonable conditions ensuring, as far as he is concerned, the security of transactions of conditional access system operators.”*

This provision supersedes the similar Article 4 (d) of the Directive 95/47/EC of the European Parliament and of the Council of October 24, 1995, on the Use of Standards for the Transmission of Television Signals (Transmission Standard Directive), Official Journal of the European Communities L 281 (Nov. 23, 1995), 51. The Transmission Standard Directive was repealed in 2002 by Article 26 of the Directive 2002/21/EC of the European Parliament and of the Council of March 7, 2002, on a Common Regulatory Framework for Electronic Communications Networks and Services (Framework Directive), Official Journal of the European Communities L 108 (Apr. 24, 2002), 33.

V.2 Competition in Complementary Markets

DRM components are not only used to protect technology platforms from competition on a horizontal level. As the following four examples will illustrate, developers of technology platforms also use DRM components to control which complementary goods can use and access the platform.

DRM in the Sony Aibo Dog

For a few years now, Sony has been marketing a robot pet dog called “Aibo”. Many programs controlling the Aibo dog are stored in a storage device (the “Sony Memory Stick”) that can be inserted into the dog. This storage device is equipped with a DRM-like copy protection mechanism. Although Sony markets various programs that extend the basic functionality of Aibo, not all Aibo owners are satisfied with what Aibo is capable of. Therefore, one particularly enthusiastic owner — known as “AiboPet” — started to write new software programs that would teach Aibo new tricks and expand its functionality. One of his most successful programs, for example, taught Aibo to dance to music. In order to write such programs, the programmer had to circumvent the copy protection technology built into the Aibo Memory Stick. In October of 2001, Sony decided to take action against this “infringement” and sent a cease-and-desist letter to the programmer, citing a violation of the anti-circumvention regulations of the DMCA.¹⁸⁹³

What is difficult about the Sony Aibo case is differentiating between the important and the unimportant. The case is relatively unimportant in so far as it deals with the question of whether a company can protect its robot product with a DRM system. The case is also relatively unimportant in so far as Sony decided to actually take action against the hacking of its robot dog.¹⁸⁹⁴ Yet, the case is of importance because it exemplifies how DRM systems can be employed to control the use of and access to technology platforms. Essentially, Aibo is a platform on top of which software applications can be built and run. If such a platform is protected by a DRM system, the platform owner can control who is able to build applications on top of the platform. This can prevent unaffiliated software developers from developing applications for the platform.

DRM in Laser Printers

Another example of this power to control complementary markets involves laser and ink-jet printers. DRM can be used to protect business models that are

¹⁸⁹³ For further information on this case, see: Labrador, David (Jan. 21, 2002): Teaching Robot Dogs New Tricks. Available at: <http://www.sciam.com/article.cfm?articleID=0005510C-EABD-1CD6-B4A8809EC588EEDF>; Harmon, Amy (Nov. 5, 2001): Compressed Data — Put Off by Disco Dancing, Sony Tightens Leash on Its Robotic Dog. N.Y. Times, Nov. 5, 2001 at C4; No New Tricks for Robot Dog, Available at: <http://www.chillingeffects.org/anticircumvention/notice.cgi?NoticeID=24> (original cease-and-desist letter sent by Sony).

¹⁸⁹⁴ Later, the company changed its attitude towards Aibo programmers and has even released a software development kit for Aibo.

based on charging subcompetitive prices for a particular product, but charging supracompetitive prices for complementary products. For a long time, printer manufacturers have been offering their printers at relatively low prices while charging high prices for toner cartridges.¹⁸⁹⁵ This strategy is advantageous to printer manufacturers as they can acquire a larger customer base due to the low price of the printers.¹⁸⁹⁶ In addition, it enables them to engage in price discrimination: high-volume printer users have to buy more toner cartridges and thereby pay a higher price for the product combination of printer and toner than low-volume users.¹⁸⁹⁷

While this strategy may be beneficial to both manufacturers and consumers,¹⁸⁹⁸ it is also problematic as the manufacturer has an incentive to foreclose competition on the cartridge aftermarket¹⁸⁹⁹ and impede innovation by unaffiliated third parties.¹⁹⁰⁰ Indeed, over the last several years, printer manufacturers have increas-

¹⁸⁹⁵ In the United States, e.g., Lexmark offers discounts of up to \$ 50 on its cartridges, see: *Lexmark International, Inc. v. Static Control Components, Inc.*, No. 02-571-KSF, at 3 (E.D.Ky. 2003), at: http://www.eff.org/IP/DRM/DMCA/Lexmark_v.Static.Controls/20030303-finding-of-facts.pdf. This strategy can be observed in other areas as well: razors are given away to sell the blades, copying machines are sold cheaply to sell the service and replacement parts — a tactic which may lead to antitrust concerns, see: *Eastman Kodak Co. v. Image Technical Services, Inc.*, 504 U.S. 451 (1992).

¹⁸⁹⁶ See: Varian (2001): 14; Shapiro, Varian (1999): 118–121, 142–143; see also: the complaint in *Lexmark International, Inc. v. Static Control Components, Inc.*, 4, at: <http://www.politechbot.com/docs/lexmark.complaint.010803.pdf> (Dec. 30, 2002): “*Lexmark’s strategy is based on a business model of building an installed base of printers that will then generate demand for Lexmark’s printer supplies and services.*”

¹⁸⁹⁷ See: Pindyck, Rubinfeld (2001): 402; Varian (2001): 14, 16. For a general analysis of price discrimination in proprietary aftermarkets, see: Emch (2003). For an opposing analysis of creating customer lock-ins through proprietary aftermarkets, see: Borenstein, MacKieMason, Netz (2000). In order to prevent customers from having their low-price cartridges refilled by a third-party cartridge manufacturer, Lexmark attaches a shrink-wrap license to its low-price cartridge. According to this license agreement, customers are allowed to use the cartridge only once. When the cartridge is empty, they are required to return the cartridge to Lexmark. See: *Lexmark International, Inc. v. Static Control Components, Inc.*, No. 02-571-KSF, at 3 (E.D.Ky. 2003), *supra* note 1895. Shrink-wrap licenses are often used to support price discrimination and prevent arbitrage. See e.g.: *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447, 1449–1450 (7th Cir. 1996).

¹⁸⁹⁸ See: Varian (2001): 14. For more information on the rather complex economics of laser printer toner cartridges, see: Emch (2002).

¹⁸⁹⁹ See: Varian (2001): 16; see also: *Eastman Kodak Co. v. Image Technical Services, Inc.*, 504 U.S. 451 (1992). However, whether the foreclosure of aftermarkets leads to antitrust and competition policy concerns depends on the underlying theoretical economic framework. For an assessment of how the Kodak decision of the Supreme Court marks the transition from Chicago School to Post-Chicago School economics, see: Lande (1993); see also: Posner (2001): 236–237; Hovenkamp (1993); Klein (1993); Emch (2002/2003); Borenstein, MacKieMason, Netz (2000).

¹⁹⁰⁰ As Varian (2002) points out, embedding DRM technologies into ink-jet printers could impede innovative uses of the printers that were not envisioned by

ingly used DRM-related technologies to prevent third-party cartridge manufacturers from entering the cartridge aftermarket with low-priced cartridges. Today, companies such as Hewlett-Packard and Lexmark include sophisticated security chips in their printers to control the data flow between the printers and the toner cartridges. These security systems include challenge-response protocols, encryption systems, secure hashing algorithms, radio communication, custom-designed chips, and custom-designed communication protocols as well as periodic firmware updates, all of which are used to detect toner cartridges that are produced by third-party manufacturers.¹⁹⁰¹ If such a toner cartridge is detected, the printer ceases operation.

In February 2003, in a case that could have significant impact on the whole remanufacturing industry, a U.S. district court in Kentucky issued a preliminary injunction against a company called Static Control Components (SCC).¹⁹⁰² SCC produces microchips that can be installed in third-party toner cartridges. Equipped with these microchips, the toner cartridges can be used in Lexmark laser printers. Although the Lexmark printers try to detect unauthorized toner cartridges by using access control technologies, third-party toner cartridges that are equipped with the SCC microchip can be used in the printers as the microchip circumvents the access control that resides in the printers. As the availability of cheap toner cartridges from third-party vendors threatens Lexmark's business model, Lexmark wanted to force SCC to stop manufacturing its chips. In the preliminary injunction, the district court accepted Lexmark's line of argument and ruled that SCC's chips violated section 1201 (a) (2) of the DMCA as they circumvent an access control that is implemented in a software program located in the printer.¹⁹⁰³

By using DRM technology and anti-circumvention regulations, Lexmark intended to protect a technology platform (the printer with the access control software running on it) from competitors in complementary markets (the toner

the printer manufacturer, such as using magnetic ink to squirt integrated circuits onto metalized plastic – a technology that could revolutionize integrated circuit production. For an analysis of the importance of enabling consumers to innovate on the basis of mass-market products, see: Hippel, Katz (2002); Thomke, Hippel (2002). This is an example of how increasing technological and intellectual property protection may lead to a concentration and homogenization of innovation; see *infra* text accompanying note 1923.

¹⁹⁰¹ See: Static Control Components, Inc., Computer Chip Usage in Toner Cartridges and Impact on the Aftermarket: Past, Current and Future, available at: <http://www.scc-inc.com/special/oemwarfare/whitepaper/default.htm> (last modified Feb. 13, 2003); see also: Complaint in Lexmark International, Inc. v. Static Control Components, Inc., 6–8, *supra* note 1896.

¹⁹⁰² See: Lexmark International, Inc. v. Static Control Components, Inc., No. 02-571-KSF (E.D.Ky. 2003), *supra* note 1895.

¹⁹⁰³ See *Id.*: 39–43. The court also opined that SCC's actions were not exempted from liability by the reverse-engineering clause of 17 U.S.C. § 1201 (f), see *Id.*: 47–48. In January 2003, Static Control Components proposed to the U.S. Copyright Office to create an exemption to the DMCA's anti-circumvention provisions so that Lexmark and other printer vendors could no longer use the DMCA to control the cartridge aftermarket, see: <http://www.copyright.gov/1201/2003/petitions/static.pdf> (Jan. 23, 2003).

cartridges market).¹⁹⁰⁴ Similar examples of this strategy include car manufacturers protecting software routines by DRM technology so as to prevent competition in the aftermarket for replacement tires, wiper blades or other automotive parts,¹⁹⁰⁵ Microsoft allowing software to be run on its Xbox game console only after the software has been signed by Microsoft,¹⁹⁰⁶ or cell phone manufacturers applying DRM technology to replacement batteries, headsets or car adapters.¹⁹⁰⁷

¹⁹⁰⁴ While, in the U.S., this raises question of the applicability and scope of the anti-circumvention regulations of the DMCA, European legislation and administration attempt to address the problem in other ways. Firstly, according to news reports, the European Commission is considering an investigation of the European printer market from an antitrust perspective. Secondly, the recently adopted European Directive on Waste Electrical and Electronic Equipment (WEEE) includes a provision according to which printer manufacturers are forbidden to use DRM systems to prevent toner cartridges from being re-filled and re-used; see: Article 4 of the Directive 2002/96/EC of the European Parliament and of the Council of January 27, 2003, on Waste Electrical and Electronic Equipment (WEEE), Official Journal of the European Union L 37 (Feb. 13, 2003), 24; see also: Report of the European Parliament Delegation to the Conciliation Committee, Document A5-0438/2002 (Dec. 5, 2002), 11. Although this provision is based on recycling considerations, it could also open competition in the toner cartridge market.

¹⁹⁰⁵ For some information on the corresponding European legal framework, see: Article 4 (2) and Recital 26 of the Commission Regulation (EC) No. 1400/2002 of July 31, 2002, on the Application of Article 81 (3) of the Treaty to Categories of Vertical Agreements and Concerted Practices in the Motor Vehicle Sector, Official Journal of the European Communities L 203 (1.8. 2002), p. 30. For some information on the situation in the U.S., see the letter of automobile manufacturer and service industry groups to the U.S. Senate, at: <http://www.asashop.org/legis/agreement.htm> (Sept. 20, 2002); see also: <http://www.asashop.org/legis/jointrelease.htm> (26.9., 2002); The Motor Vehicle Owner's Right to Repair Act, H.R. 2735, 107th Cong. (2001) (not enacted).

¹⁹⁰⁶ The Microsoft Xbox is basically a normal PC with some security-related and some game-specific alterations. One of these alterations includes hardware-based mechanisms that allow only software to be run on the Xbox that has been issued a digital certificate by Microsoft; see: Bartholomew (2002); Lehner (2002); Green (2003); Huang (2002a). The Xbox Linux project is trying to create a version of the Linux operating system that could be run on the Xbox. Without any reverse engineering, this could only be achieved if Microsoft signed this particular version of Linux for use on the Xbox. Microsoft has never replied to the requests of the Xbox Linux project to issue such a certificate; see: *Microsoft Approval Sought for Xbox Linux Project* (Feb. 24, 2003), at: <http://www.theregister.co.uk/content/54/29439.html>; <http://xbox-linux.sourceforge.net/articles.php?aid=20030047001211>; <http://xbox-linux.sourceforge.net/articles.php?aid=20030062171641>. According to news reports, Microsoft sells the Xbox below costs and, at least in the beginning, lost as much as \$ 110 on every box sold; see: Gaither, Chris: Microsoft Cuts Xbox Price. N.Y. Times, May 15, 2002, at C4; O'Brien (2001): 46. Therefore, Microsoft's attempt to enter the game console market can only be successful if consumers spend enough money in the complementary game aftermarket. As a result Microsoft has strong interests in preventing consumers from buying a heavily subsidized Xbox, installing a third-party operating system and using the Xbox as a normal personal computer. Despite the security measures taken by Microsoft,

DRM in Microsoft's Operating Systems

Another example illustrating how DRM may be used to control complementary markets involves DRM-enabled computer operating systems. DRM systems that are included in operating systems do not only increase the operating systems' security, they may also be used strategically. In particular, they may be used to impede competitors' development of software or hardware that is compatible with the operating system. By keeping details of application programming interfaces (APIs) or communication protocols of a DRM system secret or undocumented, by delaying the disclosure of such information and by assigning DRM encryption keys to hardware manufacturers, software programmers, and content providers on a discriminatory basis, the developer of an operating system may control who is able to create interoperable software applications and who can protect and distribute content in this system.

Therefore, it may seem surprising that the consent decrees, which brought the U.S. antitrust proceedings against Microsoft to an end in late 2002, include "security carve-out" provisions according to which Microsoft is not required

"to document, disclose or license to third parties:

- a) *portions of APIs or Documentation or portions or layers of Communications Protocols the disclosure of which would compromise the security of a particular installation [...] of anti-piracy, [...] software licensing, digital rights management, encryption or authentication systems, including without limitation, keys, authorization tokens or enforcement criteria [...]*.¹⁹⁰⁸

The consent decrees further state that Microsoft is allowed to condition any license of any of the technologies mentioned

"on the requirement that the licensee [...]

the Xbox Linux project succeeded in creating a full Linux version that could be executed on an Xbox with hardware modifications (using a so-called "mod chip") in October 2002. In March 2003, the project reportedly succeeded in getting Linux to run on the Xbox without hardware modifications; see: Backer, David (March 31, 2003): Hackers Cracks Xbox Challenge, at: <http://news.com.com/2102-1043-997497.html>; <http://xbox-linux.sourceforge.net>.

¹⁹⁰⁷ See: Anderson (2003a): 2. For an argument of how trusted computing architectures could exacerbate the problem, see *infra* note 2065. Another case that is similar to the Lexmark case involves remote control garage door opener systems. In 2002, a U.S. manufacturer of such systems brought a lawsuit against a manufacturer of remote controls. By claiming that these remote controls circumvented the garage door opener systems' access control technologies, the plaintiff attempted to prevent the competing manufacturer from entering the complementary remote control market. For more information, see: Chamberlain Group, Inc., v. Skylink Technologies, Inc., Amended Complaint, at: http://www.eff.org/IP/DMCA/20030114_chamberlain_v_skylink_amd_complaint.pdf (Oct. 16, 2002), and Memorandum, available at: http://www.eff.org/IP/DMCA/20030113_chamberlain_v_skylink_motion.pdf (Dec. 3, 2002).

¹⁹⁰⁸ See: U.S. v. Microsoft Corp., 2002 Westlaw 31654530, at 6, § III.J (D.D.C. Nov. 12, 2002); State of New York v. Microsoft Corp., 224 F.Supp.2d 76, 272, Appendix B, § III.J (D.D.C. Nov. 1, 2002).

- b) has a reasonable business need for a planned or shipping product,
- c) meets reasonable, objective standards established by Microsoft for certifying the authenticity and viability of its business,
- d) agrees to submit, at its own expense, any computer program using such [technology] to third-party verification, approved by Microsoft, to test for and ensure verification and compliance with Microsoft specifications for use of the [technology] [...].¹⁹⁰⁹

There are legitimate reasons for such security carve-out provisions. An unconditional mandate to disclose information about Microsoft's DRM implementation could compromise its security as such information could be used to hack the DRM system.¹⁹¹⁰ Nevertheless, the security carve-out provisions in question bear the danger that Microsoft could refuse to disclose or delay the disclosure of information about its DRM architecture on technically unjustified "security" issues.¹⁹¹¹ Although the court emphasized that the consent decrees strike a balance between the legitimate interests of Microsoft and its competitors by limiting the security carve-out to relatively narrow circumstances and that the provisions do not authorize Microsoft to discriminate against competitors,¹⁹¹² it is an open question whether this particular solution of the tension between security and competition will work in practice.

Region Coding, Competition and the Free Movement of Goods

The final example which illustrates how DRM technology can be used to control complementary markets involves technologies that separate markets geographically. Most DVD players and DVD discs include a so-called "regional code playback control". This system divides the world market into six distinct geographic regions. It is able to prevent, for example, European consumers from playing U.S. DVDs on a European DVD player.¹⁹¹³ Similar systems can be found in Sony's Playstation game consoles¹⁹¹⁴ and in various software applications.

¹⁹⁰⁹ See: *Id.*

¹⁹¹⁰ See: *U.S. v. Microsoft Corp.*, 231 F.Supp.2d 144, 193–195 (D.D.C. Nov. 1, 2002); *State of New York v. Microsoft Corp.*, 231 F.Supp.2d 203, 251–252 (D.D.C. Nov. 1, 2002). Whether this statement is actually true depends on whether one believes that achieving security by secrecy or obscurity is a good engineering approach. Security by obscurity directly contradicts the widely-accepted Kerckhoff principle; see *supra* note 1848; see also: *State of New York v. Microsoft Corp.*, 224 F.Supp.2d 76, 238–239 (D.D.C. Nov. 1, 2002).

¹⁹¹¹ See also: *State of New York v. Microsoft Corp.*, 224 F.Supp.2d 76, 239 (D.D.C. Nov. 1, 2002). For a related problem in trusted computing architectures, see *infra* text accompanying note 2018.

¹⁹¹² See: *U.S. v. Microsoft Corp.*, 231 F.Supp.2d 144, 193–195 (D.D.C. Nov. 1, 2002); *State of New York v. Microsoft Corp.*, 224 F.Supp.2d 76, 239 (D.D.C. Nov. 1, 2002).

¹⁹¹³ For more information, see: Bechtold (2002): 110–112.

¹⁹¹⁴ See: *Sony Computer Entm't Am., Inc. v. Gamemasters, Inc.*, 87 F.Supp. 2d 976, 981 (N.D.Cal. 1999). Whether the circumvention of the Playstation's regional code management control actually infringes anti-circumvention regulations is not an easy question. In July 2002, an Australian federal court ruled that the

Rights holders have various legitimate reasons for using regional code management systems.¹⁹¹⁵ Nevertheless, regional code management systems in hardware¹⁹¹⁶ or software¹⁹¹⁷ platforms can also be used to exercise control over the complementary market in which digital content¹⁹¹⁸ is processed on top of the platform. Both the European and the Australian competition authorities have investigated whether the regional code management system in DVD players is used to overcharge European and Australian customers for DVD discs compared to U.S. customers.¹⁹¹⁹ Furthermore, regional code management systems can undermine the free movement of goods which intellectual property law protects by the exhaustion principle.¹⁹²⁰

Conclusion

As the four examples given illustrate, DRM technologies and anti-circumvention regulations cannot only be used to fight piracy. Rather, by wrapping technology platforms in a DRM system, DRM can be used to control downstream markets and channel innovation. How DRM policy should deal with such cases is not an easy question. On the one hand, some protection for DRM platform developers may be desirable in order to provide sufficient incentives for the development of the platform.¹⁹²¹ On the other hand, such incentive structures have to be carefully drafted and limited in order to not put too many stumbling blocks along the path to well-functioning competition and cumulative innovation.¹⁹²² Highly protective intellectual property regimes may lead to an undesired concentration,

distribution of so-called “mod chips” which circumvent the Playstation’s regional code management does not violate Australian anti-circumvention regulations, *Kabushiki Kaihsa Sony Computer Entm’t et al. v. Eddy Stevens*, (2002) F.C.A. 906. For a related case in the U.K., see: *Sony Computer Entm’t, Inc. v. Paul Owen*, 2002 Entertainment and Media Law Reports 34.

¹⁹¹⁵ See: Marks, Turnbull (2000): 213; Answer of the European Commission to Written Questions E-1509/00 and E-1510/00, Official Journal of the European Communities C 53 E (Feb. 20, 2001), 158; Bechtold (2002): 110 note 557.

¹⁹¹⁶ Such as DVD players.

¹⁹¹⁷ Such as operating systems.

¹⁹¹⁸ Such as video files or software applications.

¹⁹¹⁹ See: Answer of the European Commission to Written Questions E-1509/00 and E-1510/00, *supra* note 1915; Answer of the European Commission to Written Question E-2371/00, Official Journal of the European Communities C 103 E (Apr. 3, 2001), 138; Letter of Cecilio Madero, DG Competition of the European Commission, to Lars Gaarden, at: <http://www.eurorights.org/dvd/E-1509-comments-answer.html> (Mar. 14, 2001); Australian Competition & Consumer Commission, ACCC Consumer Express (Feb. 2002), available at: http://www.accc.gov.au/pubs/Publications/Journals/consumer_express/feb2002.htm.

¹⁹²⁰ In the context of DVDs, this is not a problem, however, as the world regions used by the regional code management system seem to be larger than the geographical areas in which intellectual property rights become exhausted. This would change, however, if the principle of international exhaustion would apply; see only: Chiappetta (2000).

¹⁹²¹ See: Samuelson, Scotchmer (2002): 1621–1622.

¹⁹²² See: *Id.*: 1625–1626.

commercialization, and homogenization of information production.¹⁹²³ Solving this tension between DRM protection by intellectual property rights and DRM competition leads to the general problem how intellectual property protection and competition policy interrelates and interacts.¹⁹²⁴ More particularly, it is troublesome that anti-circumvention regulations are increasingly used in circumstances for which they were clearly not intended.

VI DRM and Standardization

The more mature DRM technology becomes, the more efforts are made to standardize various DRM components. This section describes several legal and policy problems that emerge when DRM becomes standardized.

VI.1 Standardization by the Private Sector

DRM systems are subject to indirect network effects.¹⁹²⁵ The more content is available in a particular DRM system, the more consumers will buy equipment that is compatible with this system.¹⁹²⁶ Yet, if more consumers buy such equipment, more content will be made available for the DRM system, because demand increases. After passing a certain “tipping” point, this may lead to so-called “positive feedback” effects: while one DRM system becomes more and more dominant in the market, competing DRM systems are effectively driven out of the market.¹⁹²⁷ Network effects can lead to *de facto* standards, even monopolies in a market.¹⁹²⁸

In a market with such structures, due to significant first-mover advantages, it may be rational for a company to invest heavily in the rapid acquisition of market share as early as possible.¹⁹²⁹ However, depending on various circumstances such as size and structure of the market, it may also be more effective to create

¹⁹²³ See: Benkler (2002).

¹⁹²⁴ See only: The documents of the hearings by the Federal Trade Commission and the U.S. Department of Justice on “Competition and Intellectual Property Law and Policy in the Knowledge-Based Economy” in 2002, <http://www.ftc.gov/opp/intellect>.

¹⁹²⁵ In a market shaped by positive network effects, a consumer’s utility of a good increases with the number of other agents consuming the good, see: Katz, Shapiro (1985). With indirect network effects, the effect is mediated not by the good that is subject to the network effect, but by a complementary good; see: Shy (2001): 52. The existence, importance, and impact of network effects is controversial on a theoretical as well as an empirical level; see: Liebowitz, Margolis (1994): 149; Lemley, McGowan (1998); Bechtold (2002): 351–364.

¹⁹²⁶ This is comparable to the indirect network effects of operating systems: the more application programs are available for a particular operating system, the more consumers will buy this system; see: Shy (2001): 52. Indirect network effects also occur with computer hardware, video recorders and CD players.

¹⁹²⁷ See: Shapiro, Varian (1999): 175–179; Lemley, McGowan (1998): 496–497.

¹⁹²⁸ See: Katz, Shapiro (1994): 105.

¹⁹²⁹ See: Id.: 107; Lemley, McGowan (1998): 495, 504.

a private industry organization open to all which develops a common standard to which all market participants adhere. If the members of this organization have a significant market share their adoption of the standard may also produce the positive feedback effect described above.¹⁹³⁰ It is therefore understandable that, over the last few years, many working groups, industry organizations and standardization bodies have been created or became interested in standardizing DRM components. All these efforts attempt to contribute to a comprehensive DRM architecture that is seamlessly integrated into nearly all consumer electronics devices and computer equipment. They hope to create widely accepted DRM industry standards, because the single company or the group of companies that push the efforts have a significant market share, so that their adoption of a standard would create the positive feedback effect described above.

Examples of DRM Standards

The acronyms of DRM standardization bodies are as manifold as their number is staggering. The “Copy Protection Technical Working Group” (CPTWG), for example, played a major role in standardizing copy-protection and DRM components of the DVD disc. It is still one of the most important working groups in the DRM field.¹⁹³¹ In June 2002, the “Broadcast Protection Discussion Group” (BPDG), which is a working group of the CPTWG, issued its final report recommending the inclusion of a “broadcast flag” into digital TV broadcasting in order to forestall unauthorized copying.¹⁹³² The “Secure Digital Music Initiative” (SDMI), which was founded in 1999, started with fanfare, but failed to deliver any DRM standards that would be implemented in the market on a wide-scale basis.¹⁹³³

Since 1995, the Dublin Core Metadata Initiative has been working on a standard for a rudimentary set of metadata.¹⁹³⁴ In early 2002, OASIS — a group responsible for crafting XML interoperability standards — announced the creation of a technical committee that would standardize a rights expression language for DRM systems.¹⁹³⁵ Intel, IBM, Matsushita and Toshiba (the so-called “4C” companies) have created the “Content Protection for Recordable Media” (CPRM)

¹⁹³⁰ See: Lemley, McGowan (1998): 516. Although network effects can lead to a standards monopoly, this is not inherently bad from an economic perspective. If, in a particular market, having a single standard is more efficient than having several competing standards, then this is desirable; Id.: 497. However, in such a market, it is not guaranteed that the “optimal” standard will be adopted. Network effects can lead to a lock-in into a “suboptimal” standard that neither consumers nor producers can escape due to high switching costs and collective action problems; see: Shy (2001): 4–5; Lemley, McGowan (1998): 497 (who also point out that this begs the question what an “optimal” standard actually is).

¹⁹³¹ See: Marks, Turnbull (2000): 204–205, 208.

¹⁹³² See: Broadcast Protection Discussion Subgroup, Final Report to the Copy Protection Technical Working Group, available at: <http://www.cptwg.org/Assets/BPDG/BPDG%20Report.DOC> (3.6. 2002).

¹⁹³³ For some information on SDMI, see: Marks, Turnbull (2000): 210–211; Levy (2000).

¹⁹³⁴ See: Paskin (1999): 1218–1219.

specification which is intended to protect content when recorded on physical media such as rewriteable DVDs or memory cards.¹⁹³⁶ The “Motion Picture Expert Group” (MPEG) has been dealing with DRM-related questions since MPEG-4. Further standards in the DRM field include the “Digital Transmission Content Protection” (DTCP),¹⁹³⁷ the “High-Bandwidth Digital Content Protection” (HDCP),¹⁹³⁸ the “Content Scramble System” (CSS),¹⁹³⁹ the “Copy Generation Management System” (CGMS),¹⁹⁴⁰ the envisaged “DVB Content Protection and Copy Management” (DVB CPCM),¹⁹⁴¹ the DRM-related parts of the OpenCable specification,¹⁹⁴² the still uncertain video watermark standard for DVD players,¹⁹⁴³ and various systems of regional code playback control.¹⁹⁴⁴

More recently, two new standardization efforts have entered the arena: the Trusted Computing Platform Alliance (TCPA) and Microsoft’s Palladium initiative. Both efforts attempt to implement a “trusted computing architecture”.¹⁹⁴⁵ Such architecture uses components which ensure that a computing platform always behaves in the expected manner for the intended purpose. In particular,

¹⁹³⁵ See: <http://www.oasis-open.org/committees/rights>. Indeed, the standardization effort of a “general-purpose” REL may be the most important standardization effort in the DRM field which could have impact on areas far beyond traditional DRM, such as web services and the semantic web.

¹⁹³⁶ See: Taylor (2000): 193–195, 488–489; <http://www.4centity.com/tech/cprm>.

¹⁹³⁷ DTCP protects the transmission of digital content between different hardware components, e.g., between a computer and a digital video recorder. See: <http://www.dtcp.com>; Marks, Turnbull (2000): 208.

¹⁹³⁸ HDCP protects the transmission of digital content between a computer system and a connected monitor; see: <http://www.digital-cp.com>; Taylor (2000): 199–200, 490. In 2001, severe weaknesses in the security implementation of HDCP were demonstrated; see: Crosby et al. (2001).

¹⁹³⁹ CSS is an authentication and encryption system that was designed by Matsushita and Toshiba to prevent the making of digital copies of DVDs. In fall 1999, CSS was hacked by a software program named DeCSS. For more information on CSS, see: Taylor (2000): 481; Marks, Turnbull (2000): 205–206, 211–213; *Universal City Studios, Inc. v. Reimerdes*, 111 F.Supp. 2d, 294, 308–313 (S.D.N.Y. 2000).

¹⁹⁴⁰ See: Taylor (2000): 197.

¹⁹⁴¹ See: Digital Video Broadcasting Forum, Call for Proposals for Content Protection & Copy Management Technologies, available at: http://www.dvb.org/dvb_technology/whitepaper-pdf-docs/cfp_cp_cm.pdf (July 5, 2001).

¹⁹⁴² See: CableLabs, OpenCable POD Copy Protection System, available at: <http://www.opencable.com/downloads/specs/OC-SP-PODCP-IF-I08-021126.pdf> (Nov. 26, 2002).

¹⁹⁴³ In August 2002, the DVD Copy Control Association (DVDCCA) was unable to reach an agreement on the selection of a watermarking technology for copy and playback control in DVD players and drivers; see: Motion Picture Association of America, Content Protection Status Report III, available at: <http://judiciary.senate.gov/special/mpaa110702.pdf> (Nov. 7, 2002).

¹⁹⁴⁴ See *supra* text accompanying note 1913. For a detailed overview of DRM standards, see: Lyon (2002); Bechtold (2002): 101–126.

¹⁹⁴⁵ Anderson aptly points out that the goal of such architectures is not to be “trusted”, but to be “trustworthy”; see: Anderson (2003a): 4.

the architecture provides evidence about the integrity and authenticity of the platform to both the platform's owner and to arbitrary third parties. Thereby, this architectural approach attempts to increase trust in the computing environment.¹⁹⁴⁶ If widely implemented, trusted computing architectures could alter the IT infrastructure landscape as we currently know it in considerable ways. They also raise new DRM-related problems, which will be described in the remainder of this subsection. As overview descriptions of TCPA and Palladium are still very rare, the article will first describe the underlying technologies in some detail.

Trusted Computing Platform Alliance (TCPA)

TCPA is an industry working group that was initially formed by Compaq, Hewlett-Packard, IBM, Intel, and Microsoft in 1999 and now boasts over 200 participating companies.¹⁹⁴⁷ Based on ideas developed in the mid 1990's,¹⁹⁴⁸ its goal is to create a standard for a trusted hardware computing platform. Although it is currently primarily focused on the personal computer architecture, the TCPA specification could, in the future, also be implemented on servers and mobile devices such as music players, cell phones or PDAs.¹⁹⁴⁹

TCPA is a specification for computing platforms that creates a foundation of trust for software processes, based on a small amount of special hardware within such platforms.¹⁹⁵⁰ It enables three features that are of particular interest for DRM: it enables a secure attestation of the state of a platform, it can be used to create trusted platform identities, and it provides protected storage.

Platform State Attestation

TCPA attempts to increase trust in the computing environment. It starts from the assertion that it is impossible to rely on a software process to provide reliable information unless one can be certain that this process is working as expected.¹⁹⁵¹ Therefore, TCPA provides a mechanism by which the state of all

¹⁹⁴⁶ See: Pearson (2003): 31, 41. For more information on the goals of trusted computing, see: Id.: 4–42.

¹⁹⁴⁷ For a list of the TCPA members, see: <http://www.trustedcomputing.org/tc-paasp4/members.asp>. In April 2003, the formation of a new "Trusted Computing Group" (TCG) was announced. TCG is supposed to supersede the TCPA group, using the TCPA specifications as a starting point. For more information, see: <http://www.trustedcomputinggroup.org>. By creating a new standards body, various organizational changes and more formal structures could be introduced, such as becoming incorporated, using a RAND (reasonably and non-discriminatory) patent license policy, switching to the principle of majority rule, and introducing a logo program to signal compliance of specific implementations with TCG specifications.

¹⁹⁴⁸ See, e.g.: Arbaugh, Farber, Smith (1997). This was preceded by developments of secure systems in the military sector which started in the 1960's; see: Anderson (2001); *Kuhlmann, Gehring* within this book on page 178.

¹⁹⁴⁹ For more information on TCPA, see: <http://www.trustedcomputing.org>; Pearson (2003); TCPA (2002a); TCPA (2001): Par. 6.1; see also: Pfitzner (2003); Wintermute (2003).

¹⁹⁵⁰ See: Pearson (2003): 5.

¹⁹⁵¹ See: Id.: 236.

software applications running under a particular operating system on a particular hardware can be attested to in a trustworthy manner. This mechanism performs a series of measurements that record summaries of software that has executed (or is executing) on the platform.

As a foundation for this mechanism, TCPA introduces two so-called “roots of trust” into the PC architecture:¹⁹⁵² the “Core Root of Trust for Measuring Integrity Metrics” (CRTM) and the “Trusted Platform Module” (TPM).¹⁹⁵³ The TPM is a chip that is separate from the main processor of the PC, but is securely attached to the PC mainboard.¹⁹⁵⁴ It is a self-contained processing engine with special capabilities such as a random key number generator, a digital signature engine, a hash function, and asymmetric encryption.¹⁹⁵⁵ It can also be used to securely store arbitrary secrets.¹⁹⁵⁶ The TPM is required to be tamper-resistant.¹⁹⁵⁷ It has to resist all forms of software attacks and a specified set of hardware attacks.¹⁹⁵⁸ The CRTM, which does not have to be tamper-resistant, is typically implemented as part of the PC BIOS.¹⁹⁵⁹ It is the basis for a reliable measurement of platform integrity information.

Both the TPM and the CRTM are “roots of trust”, i.e. the only components in the platform that are implicitly trusted.¹⁹⁶⁰ The main idea behind TCPA is to gradually expand trust from these roots to other components of the platform.¹⁹⁶¹ In a typical PC booting process, this expansion of trust works as follows. If a PC starts its booting process, the CRTM inside the BIOS measures its own integrity and the integrity of the entire BIOS. It stores a condensed summary of these integrity metrics inside the TPM in a tamper-resistant “Platform Configuration Register” (PCR).¹⁹⁶² Once the integrity metrics are stored in the

¹⁹⁵² For clarity reasons, only a TCPA implementation on the PC architecture will be discussed in the following.

¹⁹⁵³ In fact, the TPM consists of the “Root of Trust for Storing Integrity Metrics” (RTS) and the “Root of Trust for Reporting Integrity Metrics” (RTR). However, these terms are rarely used; see: Pearson (2003): 63.

¹⁹⁵⁴ Often, but not necessarily, the TPM is soldered onto the motherboard. By contrast, IBM has implemented its TPM on a small daughter board that plugs directly into an LPC bus connector on the motherboard. The daughter board is equipped with several physical security features. This enables users to physically pull the TPM out of the motherboard, thereby fully disabling TCPA on their computers. See also: Pfitzner (2003): 13.

¹⁹⁵⁵ See: Pearson (2003): 30, 36, 180–201.

¹⁹⁵⁶ See *infra* text accompanying notes 1976–1985.

¹⁹⁵⁷ It is basically an enhanced smart card, see: Pearson (2003): 67.

¹⁹⁵⁸ See: Pearson (2003): 63, 68, 227. TCPA does not intend to secure the TPM against all possible hardware attacks, as such security is unachievable; see: Id.: 35. The system “*provides tamper evidence only. It provides no protection against physical threats such as simple power analysis, differential power analysis, external signals, or extreme temperature. Physical protection is assumed to be provided by the environment*”, TCPA (2002b): 16.

¹⁹⁵⁹ See: Pearson (2003): 63–64.

¹⁹⁶⁰ See: Id.: 226–228, 235. For the question why these components should be implicitly trusted, see *infra* text accompanying notes 2031–2034.

¹⁹⁶¹ See: Pearson (2003): 226.

PCR, they cannot be altered or deleted until the platform is rebooted.¹⁹⁶³ The CRTM then passes control to the BIOS, which checks the integrity of the operating system loader and stores these integrity metrics in another PCR. The BIOS then passes control to the operating system loader, which measures the integrity values of the operating system, stores this information in another PCR, and passes control to the operating system. Finally, the operating system measures the metrics of its components and of *any* software application that will be loaded onto the platform and stores this information in yet another PCR. If, subsequently, another software application is loaded, the operating system updates the integrity measurement information in this PCR.¹⁹⁶⁴

The central idea behind this approach is that each component in the platform measures the next component in the chain and stores this value in such a way that it cannot later be modified by another component.¹⁹⁶⁵ This approach ensures that each binary code is measured and recorded before it is executed. As a result, rogue software cannot hide its presence in such a platform.¹⁹⁶⁶ Effectively, TCPA enables a “chain of trust” to be constructed from the roots of trust (the CRTM and TPM) to the applications executing on the operating system.¹⁹⁶⁷

This mechanism to securely attest to the software state of a platform can be used for various purposes. Firstly, it can be used by local and remote entities to check the integrity of the platform. In a so-called “integrity challenge”, the challenger compares the *actual* state of the platform (as reported by the trusted platform in its integrity metrics) with the *expected* state of the platform.¹⁹⁶⁸ Information about the expected state can be retrieved from so-called “Validation Entities” (VEs). VEs issue certificates for software applications which state that, if this application is executed on a trusted platform, the platform will be in a particular state.¹⁹⁶⁹ If the challenger compares this information with the integrity metrics as reported by the trusted platform, he can judge whether the software has been tampered with.¹⁹⁷⁰

Secondly, the mechanism to attest a platform state can also be used to enable “secure booting”. If, during the booting process of a PC, the TPM detects that the system does not boot as it should — because, for example, it boots additional software whose security is not certain — it reports this information to a non-TCPA software component that may then stop the booting process. Secure boot

¹⁹⁶² For more information on PCRs, see: Id.: 67–68, 138–140.

¹⁹⁶³ See: Id.: 36.

¹⁹⁶⁴ See: Id.: 75, 235.

¹⁹⁶⁵ See: Id.: 87.

¹⁹⁶⁶ It is questionable, however, whether this also holds true in the context of data that is executed under scripting languages such as VBScript; see, e.g.: Vaughan–Nichols (2003): 18–19 (citing Ross Anderson).

¹⁹⁶⁷ See: Pearson (2003): 72, 225–238.

¹⁹⁶⁸ See: Id.: 76–77.

¹⁹⁶⁹ See: Id.: 235. More accurately, VEs are third parties responsible for certifying that, if a software application is executed, a particular integrity (i.e. hash) value is measured and reported on the platform; see: Id.: 243.

¹⁹⁷⁰ See: Id.: 244.

makes sure that a computer system is either booted into a secure software state or that it is not booted at all.¹⁹⁷¹

Trusted Identities

TCPA also enables the creation of trusted identities. Although each TCPA-enabled PC contains a unique “endorsement certificate”, this is not used for identification purposes.¹⁹⁷² Rather, users of a TCPA-enabled PC may create several pseudonymous identities by receiving certificates from so-called “Privacy Certification Authorities” (Privacy-CA).¹⁹⁷³ If a user possesses several such identities, they can only be correlated among each other by the Privacy-CA that issued the identities. No one else has enough information to correlate trusted platform identities.¹⁹⁷⁴

As the user can choose between competing Privacy-CAs, the TCPA expects that he will be able to choose a Privacy-CA which does not correlate his various identities under any circumstance. Therefore, the TCPA argues that its architecture protects privacy interests to the largest extent possible.¹⁹⁷⁵

Protected Storage

Finally, TCPA enables protected storage. The TPM is a secure portal to potentially unlimited amounts of protected storage.¹⁹⁷⁶ In the tamper-resistant TPM chip, a so-called “Storage Root Key” (SRK) is stored. The SRK¹⁹⁷⁷ is never revealed outside the TPM. It can be used to securely encrypt and decrypt arbitrary data, including content and encryption keys (so-called “TPM protected objects”).¹⁹⁷⁸

In regards to DRM, three features of protected storage are important to highlight: Firstly, a TPM protected object can be “sealed” to a particular software state on a platform. As a result, the object can only be accessed if the platform is in an agreeable state.¹⁹⁷⁹ This makes it possible to restrict the conditions

¹⁹⁷¹ See: Id.: 90, 140. Yet, secure boot is not the normal operation of TCPA. Rather, a TCPA platform normally uses an “authenticated boot process”, in which the platform could end up in any arbitrary state, but that state will be recorded and can be reported; see: Id.: 90.

¹⁹⁷² But it is used in the creation of trusted identities, see *infra* text accompanying note 2059.

¹⁹⁷³ See: Id.: 80–84; see also: Arbaugh (2002): 78; Pfitzner (2003): 13. The TCPA specification also allows users to create various identities with different Privacy-CAs; see: Pearson (2003): 233.

¹⁹⁷⁴ See: Pearson (2003): 62, 78, 82.

¹⁹⁷⁵ See: Id.: 31–32, 82; but see *infra* text accompanying notes 2057–2064.

¹⁹⁷⁶ See: Id.: 38, 85, 145–146.

¹⁹⁷⁷ More precisely, the private key part of the asymmetric SRK key pair, see: Id.: 85.

¹⁹⁷⁸ See: Id.: 38. The TCPA specification distinguishes between “TPM protected data objects” and “TPM protected key objects”, see: Id.: 145. The protected objects are not stored in the TPM itself; the TPM is not a memory device, but merely a portal to any storage medium, Id.: 58, 85. See also: Pfitzner (2003): 6–7.

¹⁹⁷⁹ This is done by storing the objects alongside target PCR values, which store summaries of the software state of a platform. The TPM reveals the protected

under which data can be used and accessed on a remote computer.¹⁹⁸⁰ In a DRM system, this feature could be used by content providers to make sure that their content may only be accessed by consumers if their devices are in a secure state.¹⁹⁸¹

Secondly, TCPA distinguishes between “migratable” and “non-migratable” objects. While the first kind of object can be moved to another platform, the second kind is cryptographically bound to a specific platform.¹⁹⁸² Non-migratable objects are particularly important in the DRM field as they can be used to bind content to a particular computer.¹⁹⁸³ They are locked to this computer and can never be duplicated. If, in such a system, a hacker succeeded in copying content to another computer or device, this would be futile as the content could not be decrypted on the other computer.¹⁹⁸⁴

Thirdly, in the TCPA architecture, no global secrets exist. Every trusted platform is equipped with distinct keys. If an attacker succeeds in hacking a platform, the overall security of the TCPA architecture is not compromised as other platforms are not affected by this attack.¹⁹⁸⁵ This increases the overall security of a DRM system that is built on top of TCPA.

object only if the current PCR values match the PCR values that are stored with the object; see: Pearson (2003): 48, 87, 153.

¹⁹⁸⁰ See: Id.: 47.

¹⁹⁸¹ See: Id.: 87. See also: Id.: 237: “*Local components of the platform can therefore be designed to rely on the TPM’s trustworthiness to protect themselves against potential threats from their own execution environment. This in turn will allow entities external to the platform to trust that an application’s secret data can be protected to be only available when the [trusted platform] has been able to establish a given chain of trust from the start of its boot process up to the execution of the application itself. If a chain of trust is broken by integrity metrics that report unknown software, or software that does not cooperate in building the chain of trust further, the protected data [...] will not be accessible on the platform.*”

¹⁹⁸² See: Id.: 47–48, 165–178. In the case of a non-migratable object, the private key that is necessary to decrypt the non-migratable object is only known to the TPM that created the private key and is never revealed outside of the TPM; see: Id.: 86, 149.

¹⁹⁸³ See: Id.: 86–87.

¹⁹⁸⁴ Non-migratable objects can, however, be *moved* to another platform with the cooperation of the platform manufacturer, see: Id.: 168–169. Binding content to a particular device by cryptographic tools is not a novel approach. Rather, both the CPRM and CPPM standards bind content to unique storage media as well; see: Bechtold (2002): 113.

¹⁹⁸⁵ Therefore, TCPA is “BORE”-resistant (“break once, run everywhere”); see: Pearson (2003): 58, 227. This is true for Microsoft Palladium as well, see: Microsoft Corp. (2003). However, two caveats must be made. Firstly, achieving BORE-resistance is the theoretical idea. Whether this actually works out in practice, is another question. Secondly, if trusted platform manufacturers include an optional TCPA mechanism that enables a remote upgrade of their platforms, there is a danger that all platforms of each manufacturer are equipped with one common private key to initiate the upgrade process; see: Pearson (2003): 187. This could increase the overall vulnerability of the TCPA security architecture.

Microsoft Palladium

Although TCPA requires some modifications to existing operating systems,¹⁹⁸⁶ the specification does not include any standards for these software layers.¹⁹⁸⁷ One future operating system that could build upon the TCPA hardware architecture is Microsoft Palladium. While it is a slight simplification,¹⁹⁸⁸ one can think of TCPA as a standard for a tamper-resistant hardware environment, while Palladium provides a tamper-resistant operating subsystem that builds on such a hardware environment.¹⁹⁸⁹ Initially named after the mythical statue that guarded Troy, Palladium is likely to be incorporated into future versions of Microsoft Windows. Perhaps when Microsoft was reminded that, after Odysseus and Diomedes had succeeded in stealing Palladium from the temple of Athene in Troy, the Greek were able to capture the city some 3000 years ago, Microsoft announced in January 2003 to rename its Palladium project to “Next-Generation Secure Computing Base” — clearly something that did not exist in the Ancient World. Nevertheless, this article will use the former name as it is still widely used and easier to grasp than the acronym NGSCB.

Although little detailed information about Palladium is publicly available at the time of this writing,¹⁹⁹⁰ some of the rough outlines of the system are already known. Palladium is based on the idea of system compartmentalization.¹⁹⁹¹ Whereas one section of a computer’s memory is not affected by Palladium, another section is turned into a trusted space. In this space, Palladium uses two

¹⁹⁸⁶ Indeed, without appropriate support by an operating system, TCPA would not enable a secure DRM, see: Arbaugh (2002).

¹⁹⁸⁷ See: Pearson (2003): 238.

¹⁹⁸⁸ The Palladium initiative does not only address software issues, but also includes hardware components. Currently, the TCPA specification does not support all the primitives that are needed for Palladium, and the privacy model of both architectures is different. Therefore, it used to be unclear whether Palladium will actually be built on top of TCPA; see: Peter Biddle, posting to cryptography@wasabisystems.com, available at: <http://www.cl.cam.uk/~rja14/biddle.txt> (Aug. 5, 2002). Meanwhile, however, Microsoft has announced to use a future version of TCPA as a hardware foundation for Palladium; see: Microsoft Corp. (2003). The forthcoming version 1.2 of the TCPA specification will include several features to allow Palladium to be built on top of TCPA. For an overview of some of the changes that are expected in version 1.2 of the TCPA specification, see: Grawrock (2002). Nevertheless, TCPA may be used in combination with any operating system that meets the requirements of the TCPA specification; see also: *Kuhlmann, Gehring* within this book on page 178.

¹⁹⁸⁹ In the Palladium nomenclature, the tamper-resistant hardware components on which the Palladium software components build are called “Security Support Components” (SSC), see: Microsoft Corp. (2003).

¹⁹⁹⁰ See: Microsoft Corp. (2002); Wintermute (2003); Schoen (2002). This article was finished in April 2003. Therefore, the more detailed technical description of Palladium which has been announced by Microsoft for May 2003 could not be considered.

¹⁹⁹¹ System compartmentalization is a feature that distinguishes Palladium from TCPA in its current version 1.1b. For more information on system compartmentalization, see: England, Peinado (2002): 346.

components. The first component, called “Nexus” (formerly known as “Trusted Operating Root”, TOR), is essentially the kernel of the Palladium-isolated software stack.¹⁹⁹² It provides basic services to the second component, so-called “trusted agents” (also known as “Nexus Computing Agents”, NCAs). These are trusted software applications that call the Nexus for security-related services and critical general services such as memory management. Together, both components provide protected storage, binding data to particular platforms,¹⁹⁹³ secure encryption services, migratable encrypted objects, state attestation, authenticated boot facilities, and trusted pseudonymous identities.¹⁹⁹⁴

While these functionalities resemble many of the features offered by TCPA, Palladium provides some additional features that are not offered by TCPA in its current version.¹⁹⁹⁵ By using hardware-based “curtained” memory, Palladium ensures that each Palladium-aware application has its own execution memory space.¹⁹⁹⁶ Thereby, Palladium can securely isolate software applications from each other and prevent the modification of applications or the snooping of their memory space by other adversarial applications.¹⁹⁹⁷ Furthermore, Palladium creates a tamper-resistant communication path from the keyboard and mouse to software applications as well as from these applications to the computer display.¹⁹⁹⁸

In general, Palladium makes it possible to isolate software applications and store data for them while ensuring that only software trusted by the data’s owner has access to the data.¹⁹⁹⁹ These features could make Palladium very attractive to content providers who want to distribute their content in a DRM system.

DRM in a World of Trusted Computing

Although it is sometimes implied by opponents of trusted computing architectures, the foremost goals of such architectures do not have anything directly to do with DRM. Rather, trusted computing architectures could lead to a significant increase of the general IT security. The areas where such architectures could be useful are nearly innumerable.²⁰⁰⁰

¹⁹⁹² See: Microsoft Corp. (2003).

¹⁹⁹³ See: Schoen (2002) (describing the binding to a particular hardware system in the Palladium architecture).

¹⁹⁹⁴ See: Microsoft Corp. (2002/2003).

¹⁹⁹⁵ However, it is expected that the forthcoming version 1.2 of the TCPA specification will include these features so that Palladium can use TCPA as a hardware foundation.

¹⁹⁹⁶ See: Microsoft Corp (2003). For the related idea of system compartmentalization, see *supra* text accompanying note 1991.

¹⁹⁹⁷ See also: England, Peinado (2002): 346, 351.

¹⁹⁹⁸ See: Microsoft Corp (2003).

¹⁹⁹⁹ See: Id.

²⁰⁰⁰ See: Pearson (2003): 43–56, 251–276; see also: Safford (2002b); Pfitzner (2003): 10–11; but see: Anderson (2003a): 6–7 (doubting whether trusted computing will be valuable in the corporate and government sector).

Nonetheless, trusted computing architectures could be very attractive to DRM designers as they could serve as a firm foundation for a secure DRM system.²⁰⁰¹ On top of a trusted computing platform, a DRM system could use hardware-based tamper-resistant mechanisms for encryption, integrity and authenticity checking, policy enforcement and key revocation. By using curtailed memory, trusted computing platforms could isolate applications from each other so that rogue software could not snoop or modify DRM audio or video player software.²⁰⁰² This is not to say that such a DRM system would be 100% secure. But it would probably be much more secure than current software-based DRM implementations.

However, whether trusted computing architectures will actually be used as a foundation for a secure DRM system is currently not certain by any means. Firstly, as was noted above, TCPA and Palladium do not provide utmost security against hardware attacks by the local owner of the trusted platform.²⁰⁰³ At least initially, TCPA was focused on increasing security in the enterprise computing environment, where distrusting local platform owners is not the most important security concern. Therefore, even proponents of TCPA argue that TCPA is not particularly suited to DRM, which has to protect data against the local platform owner as well.²⁰⁰⁴

Secondly, if a DRM systems developer chose to use trusted computing architectures to securely attest the state of computing platforms, this could render the DRM system incredibly complex. As was described above, in a trusted system, any change to the BIOS, the operating system and any software application running on the system has to be reported in the integrity metrics storage.²⁰⁰⁵ If a content provider wanted to use these metrics to decide whether a particular platform is in a secure state so that the protected content could be transmitted to the platform, he would have to be able to interpret the countless different integrity metrics resulting from the myriad hardware platforms, operating systems, software patches, and software applications running on the platform.²⁰⁰⁶ The innumerable combinations of hardware and software components could pose a

For some of the motivations of IT companies to develop TCPA, see: *Kuhlmann, Gehring* within this book on page 178; Anderson (2003a): 8–9.

²⁰⁰¹ See: Microsoft Corp. (2003); Erickson (2003): 38–39; Anderson (2003a): 3; *Kuhlmann, Gehring* within this book on page 178. For an example of how DRM on top of TCPA might look like, see: Huang (2002): 103–104.

²⁰⁰² See: Microsoft Corp. (2003).

²⁰⁰³ Concerning TCPA, see *supra* text accompanying note 1958. Concerning Palladium, see: Microsoft (2003) (stating that Palladium “*is not designed to provide defenses against hardware-based attacks that originate from someone in control of the local machine*”).

²⁰⁰⁴ See: Safford (2002a): 3. See also: TCG (2003), FAQ no. 22 (“*It is not TCG’s intention to address DRM requirements. As a result, the specifications do not include provisions to prevent owner tampering*”); Pfitzner (2003): 16. However, this weakness may be reduced with the introduction of version 1.2 of the TCPA specification.

²⁰⁰⁵ See *supra* text accompanying notes 1960–1964.

²⁰⁰⁶ See: Safford (2002b): 5.

major stumbling block to the utilization of trusted computing platforms in the consumer sector.²⁰⁰⁷ These problems do not exist in the enterprise sector where, usually, a more limited and homogeneous set of hardware and software components is used.²⁰⁰⁸

Whether consumer-oriented DRM, on which this article focuses, will use trusted computing platforms to increase its security, is therefore an open question.²⁰⁰⁹ Furthermore, it is unclear at this time whether trusted computing will be implemented and how successful it will be in the marketplace. Therefore, one has to be careful at this time not to jump to erroneous conclusions about the implications of trusted computing in general and its relationship to DRM in particular. Despite these reservations, in the following, the article assumes that consumer-oriented DRM systems will use trusted computing platforms as their foundation. Therefore, in the remainder of this subsection, some of the DRM-related dangers arising from trusted computing architectures such as TCPA and Palladium will be discussed.²⁰¹⁰

Dangers Related to Competition Policy and Institutional Arrangement

Trusted computing platforms could be used by companies developing the hardware and software components of the platform to thwart competition.²⁰¹¹ As was described above,²⁰¹² TCPA can be used to “seal” data to a particular software state on a platform. In a DRM system, this feature could be used by content providers to make sure that their content may only be accessed by consumers if their devices are in a secure state. However, it could also be used to seal data to a particular operating system, platform configuration, or software application.²⁰¹³ Software companies could develop proprietary file formats for their

²⁰⁰⁷ Therefore, Microsoft’s plan to use system compartmentalization in order to limit the trusted space to the really security-sensitive applications seems a promising approach to reduce complexity of the trusted platform operation.

²⁰⁰⁸ But see: Anderson (2003a): 6–7 (doubting whether trusted computing will be valuable in the corporate and government sector).

²⁰⁰⁹ See also: Id.: 7 (doubting whether the increased security provided by trusted computing will actually lead to viable business models).

²⁰¹⁰ This article does not address dangers or advantages of TCPA and Palladium that are not related to DRM. For a document of strong opposition against TCPA and Palladium, see: Anderson (2003); for some valid criticism of Anderson’s paper, see: Safford (2002a); Pfitzner (2003): 21–22.

²⁰¹¹ In November 2002, the German government noted that the introduction of TCPA and/or Palladium might increase entry barriers for competing software developers, in particular for open-source developers; see: Antwort des Parlamentarischen Staatssekretärs Gerd Andres vom 26. 11. 2002 auf die Frage der Abgeordneten Dr. Martina Krogmann, Bundestags-Drucksache 15/116 vom 29. 11. 2002, S. 18, 19. The European Commission has expressed similar concerns, see: John Lettice, European Antitrust Chief Concerned over MS Palladium?, available at <http://www.theregister.co.uk/content/4/25988.html> (July 2, 2002). See also: Kleine Anfrage der CDU/CSU-Fraktion “Auswirkungen des ‘Trusted Platform Module’ und der Software ‘Palladium’”, Bundestags-Drucksache 15/660 vom 17. 3. 2003, S. 1 ff.

²⁰¹² See *supra* note 1979–1981.

²⁰¹³ See: Pearson (2003): 87.

applications, preventing competitors from building possibly superior applications that can read this file format and thereby interoperate.²⁰¹⁴ As the costs of converting files would be significantly increased,²⁰¹⁵ this could deter customers from switching to competing applications, operating systems and even hardware platforms in the first place.²⁰¹⁶ Content providers could make sure that their content is only accessible with a particular proprietary player. In general, sealed storage could hamper competition in the hardware, operating system and the software application markets. Trusted computing could prove a powerful tool to create customer lock-in and artificially increase switching costs.²⁰¹⁷

Therefore, the future DRM policy debate will deal with questions such as: Should the owner of commercial data (or the developer of a word processing software) be able to dictate one particular software environment that must exist in a platform before the data (or the files written with the word processor) can be accessed? Should he be allowed to dismiss other software environments that have comparable, fully acceptable security properties? If not, what tools should technology and the law provide to assess and compare the acceptability of software environments? Should the law prescribe that rights holders and software companies may not deny competing software environments access to their content or software if these environments have certain acceptable properties? Should the law create an interoperability requirement between different software and hardware environments (including non-trusted-computing environments)? Is there a need for a “trusted computing misuse” regulation?²⁰¹⁸

Trusted computing architectures are likely to incorporate some kind of signing, certification or evaluation procedure. While the TCPA architecture itself does not require any software code or device driver to be signed to run,²⁰¹⁹ two caveats have to be made. Firstly, as was described above,²⁰²⁰ TCPA uses “Validation

²⁰¹⁴ Arbaugh (2002): 78; Anderson (2002): 8–10.

²⁰¹⁵ As Anderson (2003a): 10, points out, such conversion might even be impossible for the owner of the files. Even if he would authorize such conversion, he could still not convert them as long as the developers of the trusted hardware and software components would not provide him with appropriate conversion tools or authorizations.

²⁰¹⁶ See: Id.: 10–11.

²⁰¹⁷ See: Id.: 9–11.

²⁰¹⁸ These questions relate to the problem discussed above how and by whom “security” should be defined in the security carve-out provisions in the Microsoft antitrust consent decrees; see *supra* text accompanying note 1911.

²⁰¹⁹ Pearson (2003): 36. TCPA does not include any central certification agency that decides whether a particular software component can be used in the TCPA framework. It also does not include any central licensing agency that decides whether a particular platform is TCPA-compliant or not. Rather, TCPA provides certain conformance requirements that establish the security requirements of TCPA implementations. These requirements are used by third-party certification authorities to vouch for the correct design and implementation of TCPA standards in a particular platform; see: Id. 208. Basically, TCPA merely provides trustworthy integrity metrics which can be used by the two parties engaged in the transaction to determine if the other platform is trusted for the intended transaction; see: TCPA (2002c): 3.

Entities” to issue certificates for software applications which state that, if the application is executed on a trusted platform, the platform will be in a particular state.²⁰²¹ Secondly, even if TCPA itself does not use signing authorities in a strict sense, an operating system that builds on top of TCPA could still condition the execution of software applications upon prior evaluation and signing procedures.²⁰²²

Although the details are still unclear, the Palladium environment is likely to incorporate some kind of signing or certification procedure for software applications as well.²⁰²³ Such certification procedure could also start from application and content providers. A content provider could, for example, state that its content may only be accessed by certain software applications that have been certified as complying with certain security requirements, or that it may only be accessed if the overall platform is in a secure state.²⁰²⁴ Such procedures would rely on an underlying certification infrastructure that provides such certificates.

Although it is still unclear how important signing and certification architectures will be in a real-world implementation of trusted computing architectures, some risks of such architectures in general should be highlighted. Any trusted platform architecture that uses signing or certification procedures in order to control which application can be executed on the platform runs the danger of using this control strategically. As such architecture may prevent a user from running an “unapproved” application, it may limit the choice of applications a user actually has, as the providers of the certification infrastructure could decide which application would be certified and which not.²⁰²⁵ Such architecture could also endanger open source software. If, for open source software to be run on a trusted platform, a certificate has to be obtained, the software would have to be re-certified each time after it has been altered and extended by an open source programmer. This re-certification may be costly, take time and be an overly bureaucratic procedure.²⁰²⁶ As open source programmers probably will not have the resources to finance such re-certification, they may decide not to work on

²⁰²⁰ See *supra* note 1969.

²⁰²¹ However, it is important to note that anyone can be a validation entity in TCPA. Validation entities need no approval or certification from TCPA to operate. TCPA merely states the format of the certificates which validation entities issue; see also *infra* text accompanying notes 2038–2039.

²⁰²² See: Pearson (2003): 36.

²⁰²³ See: Microsoft Corp. (2003).

²⁰²⁴ For an argument that, within Palladium, the locus of trust resides at application and content providers, see: Anderson (2003a): 5.

²⁰²⁵ See: Arbaugh (2002): 78. One example of this strategy is Microsoft’s denial to issue a certificate for a Linux version that could be run on the Xbox game console. It is important to note, however, that Microsoft might have legitimate reasons not to issue such a certificate; see *supra* note 1906 and the accompanying text.

²⁰²⁶ See: Anderson (2003): Par. 18; *Kuhlmann, Gehring* within this book on page 178; see also: Arbaugh (2002): 78. In the context of TCPA, the “certificate” which an open source programmer would have to obtain would be a certificate by a validation entity that enables third parties to challenge the integrity of a trusted platform on which the open source program is running.

the software program at all. The idea of cumulative innovation, which lies at the heart of the open source movement, could be thwarted by the financial hurdles created by trusted computing certification architectures.²⁰²⁷

Furthermore, signing or certification procedures could hamper attempts by competitors to reverse engineer software developed by the trusted platform developer.²⁰²⁸ If a company succeeded in reverse engineering such software in order to create an interoperable program, its program would still need a certification to be run on the platform. If the certification authority would be affiliated with the platform developer, it might deny the certificate for strategic reasons.²⁰²⁹

To put it succinctly: certification architectures in trusted platform infrastructures can be used in many anti-competitive ways. While all these predictions may sound alarming, they have to be qualified in two respects. Firstly, these dangers are not unique to trusted computing platforms. Indeed, they are just another example of how DRM systems can be used to control competition in the platform or in complementary markets.²⁰³⁰ What is new about trusted computing platforms is that they increase security significantly. Compared to a purely software-based DRM system, a trusted computing platform makes it much harder to break the security architecture. Trusted computing, in other words, does not enable market participants to thwart competition, but it increases their ability to do so.

Secondly, and more importantly, it is unclear at the moment whether these dangers will ultimately materialize. This depends, in particular, on the institutional arrangement surrounding trusted computing architectures. Consider, as an example, the TCPA specification. The architectural idea of TCPA is that, in order to enable trust in a computing platform, a root of trust²⁰³¹ has to exist in this platform. From this root of trust, a chain of trust across the layers of hard- and software can then be established. This, of course, only raises the question of why anyone should have confidence in this root of trust from which the chain of trust originates.

TCPA states that, in order to have confidence in the root of trust in a computing platform, two conditions must be met. Firstly, the standard to which the root of trust adheres has to be trustworthy itself. This means that the TCPA standards have to function exactly as they claim to function. TCPA attempts to gain this trust by delivering its standards as public documents which are open for review by both consumers and the scientific community.²⁰³²

²⁰²⁷ For an important caveat to this statement in the context of TCPA, see *infra* text accompanying notes 2037–2039.

²⁰²⁸ For an analysis of the importance of reverse engineering, see: Samuelson, Scotchmer (2002).

²⁰²⁹ In the end, certification architectures can therefore have similar effects as code obfuscation technologies; see *supra* note 1884.

²⁰³⁰ See *supra* section V of this article.

²⁰³¹ Which, in the TCPA specification, are the CRTM and the TPM.

²⁰³² See: Pearson (2003): 225. Similarly, Microsoft has announced to publish the source code of the Palladium Nexus in its Shared Source Initiative, see: the interview with John Manfredelli, available at: <http://www.microsoft.com/presspass/features/2002/jul02/07-01palladium.asp> (Jul. 1, 2002).

Even if the TCPA specification is considered trustworthy, the root of trust can only be trusted if, secondly, it is certain that the root of trust is fully compliant with the TCPA specification. Therefore, TCPA requires five certificates by four different logical entities that certify that a particular platform is in fact a genuine trusted platform that fully complies with the TCPA specification.²⁰³³

From an abstract perspective, what TCPA ultimately does is that it changes the targets in which computer users and third parties have to trust. They do not have to trust in any of the components of computing platforms any more. Rather, they have to trust in certain institutions which vouch for the security of particular computing platforms. The TCPA architecture then transfers this *trust in entities to trust in components*.²⁰³⁴ If TCPA succeeds, it will reduce the areas in which computer users have to trust to a few well-defined institutions and documents.

In such an approach, which is common to all trusted computing architectures, it becomes of utmost importance how these institutions are designed. One possible institutional arrangement would be to use a centralized agency that provides all certifications. Another institutional arrangement would be to allow competition to occur among different agencies that provide certification services.²⁰³⁵ If well-functioning competition between different certification agencies existed, many of the problems raised above would be solved by market forces.²⁰³⁶ Consider, for example, the potential tension between open source software and TCPA that was

²⁰³³ These entities are the “Trusted Platform Module Entity” (TPME) (vouching that the TPM is genuine, i.e. that it contains a genuine “endorsement key”), the “Conformance Entity” (CE) (issuing two certificates which vouch that the design of a particular class of platform meets the requirements of the TCPA specification), the “Platform Entity” (PE) (vouching that a specific platform is an instance of a class of platforms that meets the TCPA specification), and the “Privacy-Certification Authority” (Privacy-CA) (vouching that a particular identity belongs to a trusted platform). In addition, “Validation Entities” (VE) are used to vouch for the expected metrics for platform components such as software applications; see Pearson (2003): 59–62, 125–131, 205–212, 226–234; Kuhlmann, Gehring within this book on page 178.

²⁰³⁴ See: Pearson (2003): 234.

²⁰³⁵ Microsoft claims to use the second institutional arrangement in Palladium; see: Microsoft Corp. (2002) (stating that “[a]nyone can certify ‘Palladium’ hardware or software, and it is expected that many companies and organizations will offer this service. Allowing multiple parties to independently evaluate and certify ‘Palladium’-capable systems means that users will be able to obtain verification of the system’s operation from organizations that they trust. In addition, this will form the basis for a strong business incentive to preserve and enhance privacy and security”). TCPA enables competition among certification institutions as well. A third institutional arrangement would be to enable a fully decentralized system in which certificates are issues on a peer-to-peer basis. For an abstract analysis of how such different architectures of the certification infrastructure influences legal and policy values, see: Bechtold (2003b): 1268–1285.

²⁰³⁶ This is not to say that, in a trusted computing infrastructure, all competition-related problems could easily be solved by market forces. Even in an otherwise competitive market, without government intervention, many of the concerns

described above.²⁰³⁷ Although the financial and bureaucratic hurdles of certification and recertification could severely impede the development of open source software, this holds true only if a monopolistic or oligopolistic certification infrastructure would exist. At least theoretically, however, TCPA allows every software developer to become his own certification authority.²⁰³⁸ Open source developers do not necessarily depend on any third-party certification infrastructure, but could build their own infrastructure. As long as users and other developers would trust this open source certification infrastructure, it would work without any problems in TCPA.²⁰³⁹

Using the invisible hand of competition in the certification infrastructure to solve policy problems of trusted computing architectures assumes, however, that such competition will actually work. Whether this is a valid assumption depends on many factors, including the existence of network effects, interoperability requirements and the particular design of the infrastructure. Although network effects could lead to a monopolization in the certification market, two caveats should be made. Firstly, interoperability and interconnection requirements between different certification services could decrease the adversary impacts of network effects.²⁰⁴⁰ Secondly, even if a particular certification service provider became dominant in the trusted computing certification market due to network effects, this would still not hinder users to use competing certification services as well, at least as long as the user's trusted platform would concurrently accept certificates from different certification authorities. As long as the trusted platform owners are able to use various certification services concurrently, network effects would therefore not foreclose entry into the certification market.²⁰⁴¹

related to switching costs and consumer lock-ins (see *supra* text accompanying notes 2012–2017) are likely to continue to exist. These problems could only be solved by interoperability and interconnection requirements; see also: Bechtold (2003b): 1273–1281.

²⁰³⁷ See *supra* text accompanying note 2026.

²⁰³⁸ Or, more precisely, his own validation entity. Therefore, it is possible that no commercial third-party validation entity would be needed in a future TCPA environment, as all developers of software (open source *and* proprietary) would act as their own validation entity.

²⁰³⁹ See also: Arbaugh (2002): 78. Therefore, in the context of TCPA, the sticking point is not whether proprietary validation infrastructures will impede the development of open source software, but, firstly, whether the open source community will succeed in creating its own validation entities and, secondly, whether users and other developers will trust these validation entities.

²⁰⁴⁰ For an abstract analysis of the relationship between network effects and interoperability/interconnection requirements, see: Bechtold (2003b): 1273–1281. For some general literature of network effects, see *supra* note 1925.

²⁰⁴¹ This, in turn, does not only depend on the assumption that users will be able to use various certification services concurrently, but also that they will actually do so. Unfortunately, it is highly questionable whether one can expect ordinary trusted platform users to deviate from the standard settings about certification authorities in their platforms. Both a theoretical analysis and practical examples seem to argue against this notion. On the theoretical side, steep learning curves, high transactions costs, information asymmetries (as in the “market for

In general, it is important to ensure that the certification infrastructure of trusted computing architectures is designed in a way that certification agencies do not act strategically, that independent agencies exist, and that they issue certificates on a non-discriminatory basis. In order to really have confidence in a trusted computing infrastructure, a neutral certification infrastructure, on which the trusted computing infrastructure builds, has to exist.

Until now, the companies developing TCPA and Palladium have not been actively involved in discussing the impacts of trusted computing on competition. As with earlier DRM technologies, they seem to take the view that they are mere developers of technology that should not openly engage in policy discussions. While it is highly questionable whether this is a good strategy,²⁰⁴² all the more it is important to start such discussions in legal and policy circles.²⁰⁴³

Dangers Related to Copyright Law

Although DRM systems which are based on trusted computing architectures may come into conflict with copyright law, these conflicts are hardly novel or restricted to trusted computing. In most cases, they are general problems that may occur in any DRM system.²⁰⁴⁴ Three examples may illustrate this point. Firstly, as was described above, trusted computing architectures enable content to be cryptographically bound to a particular platform, even to a particular platform configuration.²⁰⁴⁵ If copyright limitations allow a consumer to copy content to another device without the rights holder's permission, the trusted platform could nevertheless prevent such copying as the sealed content could not be decrypted on the other device. Trusted computing platforms may there-

lemons", see: Bechtold (2002): 339–344), as well as bounded rationality and willpower (see: Korobkin (2003); Jolls, Sunstein, Thaler (1998): 1477–1479) all seem to imply that users do not make informed decisions about which certification authorities to use. On the empirical side, in the context of the Platform for Privacy Preferences (P3P), it seems that most users rarely customize their browsers' privacy settings; see: Cranor (2002): 257–259; Garfinkel (1998): 44, 46. See also: Schwartz (2000): 754 (comparing the P3P example to the "blinking twelve" problem with video recorders and stressing the importance of good interface design in this context); Bechtold (2003b): 1277 note 159 (describing a similar problem in the context of local Internet browser settings on certification authorities for the Secure Socket Layer (SSL) encryption); Mackay (1991) (describing an empirical study of software customization in a Unix environment); but see: Page et al. (1996) (describing an empirical study in which 92% of the participants customized their word processing software in some way). If it is indeed unrealistic to expect users to customize the settings in their trusted platform according to their actual preferences, a well-functioning competition between different certification authorities might be unrealistic as well. Ultimately, this is just an application of the general problem what the implications of standard settings in distributed computing environments are.

²⁰⁴² See also: Landesbeauftragter für den Datenschutz Mecklenburg-Vorpommern (2003); *Kuhlmann, Gehring* within this book on page 178.

²⁰⁴³ See also: *Kuhlmann, Gehring* within this book on page 178.

²⁰⁴⁴ For a general analysis of the tension between DRM and copyright law, see: Bechtold (2002/2003a).

²⁰⁴⁵ See *supra* text accompanying notes 1979–1984, 1993.

fore come into conflict with traditional copyright law.²⁰⁴⁶ However, this is not a feature that is unique to trusted computing platforms. The CPRM/CPM standards²⁰⁴⁷ are able to bind content to particular devices as well.²⁰⁴⁸ Furthermore, even software-based DRM systems are able to prevent content from being copied to other devices.

Secondly, Microsoft Palladium offers a tamper-resistant communication path between different system components in a PC.²⁰⁴⁹ Furthermore, by using “curtained” memory, it can securely isolate software applications from each other and prevent any snooping by adversarial applications.²⁰⁵⁰ However, such ideas are not absolutely novel either. DRM standards such as HDCP²⁰⁵¹ and DTCP,²⁰⁵² for example, protect communication paths between different system components and between different devices as well.

Finally, the combination of trusted computing architectures and anti-circumvention regulations may impede security testing and research. As was described above, in a trusted computing architecture, users only have to trust in certain institutions which vouch for the security of particular computing platforms. Trusted computing architectures then transfer this trust in entities to trust in components.²⁰⁵³ While this may sound very promising at first glance, the dangers of this approach have to be considered as well. It may become hard for independent security research to assess the security of trusted platform architectures. Not only might their various technological protection measures impede security research, but breaking some of the protection measures in order to engage in security research could also violate anti-circumvention regulations. Ultimately, trusted platforms could represent a move from a security paradigm according to which security can only be guaranteed if it has been proven by independent security research to a paradigm according to which security can be guaranteed by the security architecture itself. While this move from *security by proof* to *security by trust*²⁰⁵⁴ may be troublesome, the underlying impediment of independent security research is not novel either. Rather, it is just an application of the general tension between DRM technology, anti-circumvention regulations and security research.²⁰⁵⁵

In general, trusted computing platforms do not create qualitatively new challenges to copyright law. What is novel about trusted computing is that it provides much higher security and thereby makes the circumvention of the security

²⁰⁴⁶ See: Arbaugh (2002): 79, who proposes a modification of the TCPA specification that would enable individuals themselves to authorize various devices under their control to view purchased content; see also: Huang (2002): 104.

²⁰⁴⁷ For more information, see *supra* text accompanying note 1936.

²⁰⁴⁸ See *supra* note 1984.

²⁰⁴⁹ See *supra* text accompanying note 1998.

²⁰⁵⁰ See *supra* text accompanying notes 1996–1997.

²⁰⁵¹ See *supra* note 1938.

²⁰⁵² See *supra* note 1937.

²⁰⁵³ See *supra* text accompanying note 2034.

²⁰⁵⁴ The author is indebted to Volker Grassmuck for this insight.

²⁰⁵⁵ See *supra* section II.4: *DRM and Research*.

system much more difficult than ordinary DRM systems.²⁰⁵⁶ Therefore, the potential tension between DRM systems, which are based on trusted computing architectures, and copyright law becomes much stronger.

Dangers Related to Privacy Laws

Finally, DRM systems based on trusted computing architectures may come into conflict with legitimate privacy interests. As was described above, TCPA includes an extensive infrastructure of Privacy Certification Authorities intended to protect the user's privacy.²⁰⁵⁷ However, doubts have been raised whether, from a technical perspective, the system is actually as privacy-protecting as TCPA claims it to be. One issue of concern is, for example, that the public key of the endorsement key pair, which uniquely identifies a particular trusted platform,²⁰⁵⁸ is used in the creation of trusted identities²⁰⁵⁹ — making it easier for Privacy-CAs to correlate several trusted identities and identify individual users.²⁰⁶⁰ Furthermore, for performance and financial reasons, the TCPA specification allows platform manufacturers to generate endorsement keys outside a TPM and then inject them into an individual platform.²⁰⁶¹ Although the TCPA specification mandates that injected keys must be as secure and as private as those generated inside the TPM,²⁰⁶² the risk remains that external copies of the endorsement key exist.²⁰⁶³ In general, the privacy design of TCPA heavily relies on the trustworthiness of Privacy-CAs and hardware manufacturers. As with the competition-related concerns, the implications of trusted computing for privacy protection heavily depend on the architecture of the underlying privacy certification infrastructure.²⁰⁶⁴ As was described above, TCPA's privacy model builds upon the assumption that competition between different Privacy-CAs will enable users to choose a Privacy-CA which fits their individual preferences. Unfortunately, only a real-world implementation of trusted computing architectures will show whether they will adequately protect the privacy interests of their

²⁰⁵⁶ Another novelty is the attempt to create a pervasive security infrastructure; see *infra* text accompanying note 2065.

²⁰⁵⁷ See *supra* text accompanying notes 1972–1976.

²⁰⁵⁸ See *supra* text accompanying note 1972.

²⁰⁵⁹ See: Wintermute (2003): Par. 2.6.5, see also: Arbaugh (2002): 79; Pfitzner (2003): 11–14; Pearson (2003): 124, 128.

²⁰⁶⁰ See: Pfitzner (2003): 11–12; Landesbeauftragter für den Datenschutz Mecklenburg–Vorpommern (2003): 4. As Arbaugh (2002): 79, points out, this problem could only be solved if a method existed that would be able to verify the compliance of a particular trusted platform with the TCPA specification without releasing the compliant device's identity information; see also: Safford (2002a): 5.

²⁰⁶¹ See: Pearson (2003): 124.

²⁰⁶² See: Id.: 124, 126.

²⁰⁶³ See: Pfitzner (2003): 11.

²⁰⁶⁴ See: Konferenz der Datenschutzbeauftragten, available at: <http://www.datenschutz.mvnet.de/beschlue/ent65.html>; Landesbeauftragter für den Datenschutz Mecklenburg–Vorpommern (2003) (both documents are statements of German data protection authorities on the implications of TCPA and Palladium for privacy).

users. In some usage contexts, competition among different Privacy-CAs with different levels of privacy protection might solve the privacy-related problems of TCPA. In other contexts, however, the necessary reliance upon external entities that purport to protect the user's privacy might be unacceptable.

The Peril of Pervasiveness

Many of the potential dangers described above are not unique to trusted computing. They have emerged in other contexts before. What is novel about trusted computing is that it provides much higher security and therefore increases the tension between technology and public policy values considerably. What is novel as well is the goal of trusted computing to create a security infrastructure that becomes as wide-spread as possible. Ideally, this infrastructure would not only cover personal computers, but would also extend to other computing devices such as PDAs, cell phones and mobile devices.

Trusted computing aims at creating a pervasive infrastructure. With trusted computing, any tension between technology and public policy, which might have existed before in small, well-defined subsections of the computing environment, could now become projected onto the entire computing infrastructure that surrounds us. While the tension between technology and public policy used to be restricted to isolated incidents, trusted computing could make this tension omnipresent.²⁰⁶⁵ Pervasive technology standards which nobody can evade have to be subject to close scrutiny.

Nevertheless, as the discussion of trusted computing architectures shows, many of the potential problems raised by such architectures can be solved by a clever design of the technical architecture or the institutional arrangements surrounding the architecture. Fortunately, as trusted computing architectures are still in the development stage, there may be a realistic chance to influence such architectures so that they become a neutral infrastructure which enables competition, respects copyright limitations, and protects privacy interests.

VI.2 Standardization by the Legislature or the Administration

DRM technology does not only become standardized by market participants. Increasingly, legislators are thinking about mandating the implementation of various DRM components into consumer devices. They are pushed towards adopting such laws by powerful lobbying groups from the content industries (in particular the movie industry), while most computer and device manufacturers fiercely oppose such attempts. As is often the case in the DRM debate, both sides argue with extreme scenarios. Without any mandated DRM solution, the proponents argue, cultural production as we currently know it could come to an end. The

²⁰⁶⁵ See also: Stallman (2002a): 115. The attempt of platform developers to control complementary aftermarkets (see *supra* section V.2 *Competition in Complementary Markets*) may illustrate this point. In a world of trusted computing, security primitives are available to platform developers at very low costs. This could make it rather straightforward for all sorts of vendors to control complementary aftermarkets. See: Anderson (2003a): 3.

opponents argue that a mandated DRM solution would mean the end of the general purpose computer which could have severe impacts on innovation and growth in the technology sector.²⁰⁶⁶

Traditionally, attempts by the legislators to mandate particular DRM systems have been rare, albeit not unknown. In the United States, the Audio Home Recording Act of 1992 requires consumer DAT players to be equipped with the “Serial Copy Management System” (SCMS).²⁰⁶⁷ The Digital Millennium Copyright Act of 1998 requires analog consumer video recorders and cameras to be equipped with copy protection mechanisms developed by Macrovision.²⁰⁶⁸ European Directives have been mandating, for competition policy reasons, a particular scrambling algorithm to be implemented into digital pay TV systems since 1995.²⁰⁶⁹

Nevertheless, in general, it has been a worldwide accepted policy that legislators should refrain from interfering in the DRM development process by mandating a particular system. Both the U.S. Digital Millennium Copyright Act and the European Copyright Directive of 2001 provide in so-called “no-mandate clauses” that device manufacturers are not required by law to include any DRM system into their products.²⁰⁷⁰

Yet, over the last two years, new proposals for legislative DRM mandates have emerged. For example, in the United States, in the fall of 2001, a bill called “Consumer Broadband and Digital Television Promotion Act” (CBDTPA)²⁰⁷¹ was proposed that would empower the FCC to issue a rule mandating the implementation of particular DRM standards into a broad range of digital devices. In August 2002, the FCC issued a Notice of Proposed Rulemaking aimed at mandating the recognition by digital TV consumer equipment of a “broadcast flag” developed by the “Broadcast Protection Discussion Subgroup” (BPDG) of the CPTWG.²⁰⁷² In December 2002, the U.S. cable and consumer electronics industries reached an agreement for a national digital cable TV standard. If the

²⁰⁶⁶ See: Grassmuck (2002): 36–37; see also: Marks, Turnbull (2000): 203–205.

²⁰⁶⁷ 17 U.S.C. § 1002 (a). Similar lobbying attempts to mandate SCMS in European DAT players failed. For some background, including the history of the Athens Agreement, see: Bechtold (2002): 244–245.

²⁰⁶⁸ 17 U.S.C. § 1201 (k).

²⁰⁶⁹ See: Annex VI No. 1 to the Directive 2002/22/EC of the European Parliament and of the Council of March 7, 2002, on Universal Service and Users’ Rights Relating to Electronic Communications Networks and Services (Universal Service Directive), Official Journal of the European Communities L 208 (Apr. 24, 2002), 51. This provision supersedes Article 4 (a) of the Transmission Standard Directive, *supra* note 1892. See also: Bechtold (2002): 241–243.

²⁰⁷⁰ See: 17 U.S.C. § 1201 (c) (3); Recital 48 of the European Copyright Directive, *supra* note 1852, at 14.

²⁰⁷¹ S. 2048, 107th Congress (2002). The bill was first proposed as the “Security Systems Standards and Certification Act” (SSSCA) and is sometimes referred to as the “Hollings bill”, after Senator Fritz Hollings who introduced the bill into Congress.

²⁰⁷² See: *In the Matter of Digital Broadcast Copy Protection*, 17 F.C.C.R. 16027 (F.C.C. 2002). For more information on the BPDG, see *supra* note 1932.

agreement is approved by the FCC, every digital television set in the United States would be required to be equipped with the “High-Bandwidth Digital Content Protection” (HDCP).²⁰⁷³

At first sight, mandating DRM standards seems a promising approach for a market characterized by network effects. One common DRM architecture could be introduced into the market in a relatively short period of time, and standard wars between incompatible standards could be avoided.

However, history argues against legislative DRM mandates. Given the modest success of earlier attempts to mandate DRM technologies by law, it seems not very likely that a general mandate to implement DRM components into nearly all consumer equipment will be enacted in the near future.²⁰⁷⁴ Considering the failure in Europe to even mandate the use of SCMS in consumer DAT players,²⁰⁷⁵ such a scenario seems particularly unlikely in Europe. Furthermore, all recent efforts to mandate DRM technology on a broad scale have met with fierce opposition from various groups such as the computer and consumer electronics industry²⁰⁷⁶ and consumer advocacy groups. However, industry-specific attempts to mandate DRM technology into particular families of devices (such as pay TV decoders or mobile players) may prove much more successful in receiving the necessary support for a legislative adoption.

It is not only history that makes broad legislative or administrative DRM mandates unlikely. Forcing the inclusion of DRM technology components into the general PC hardware could mean the end of the general purpose computer as we know it: the PC owner would lose his “freedom to tinker” with his own hardware, as Edward Felten calls it.²⁰⁷⁷ The eradication of the general-purpose PC could have an unforeseeable negative impact on innovation and commercial development in the computer industry.

While these are valid concerns, technological mandates create other kinds of problems as well. One should not forget that DRM benefits primarily content providers. Therefore, it seems only a second-best solution to create a statutory DRM mandate, as this would assign the costs of DRM implementation not to content providers, but to technology vendors. Furthermore, legislative standardization runs the risk of freezing outdated or inherently insecure tech-

²⁰⁷³ See: *Consensus Cable MSO — Consumer Electronics Industry Agreement on “Plug & Play” Cable Compatibility and Related Issues*, *supra* note 1833. See also: Taub, Eric A.: *Pact Lifts an Obstacle to HDTV Transition*, N.Y. Times, Jan. 2, 2003, at G7. For more information on HDCP, see *supra* note 1938.

²⁰⁷⁴ See also: Netanel (2003): 10–11; Samuelson (2003).

²⁰⁷⁵ See *supra* note 2067.

²⁰⁷⁶ See only: Technology and Record Company Policy Principles, available at: http://www.bsa.org/usa/policyres/7_principles.pdf (Jan. 2003) (in which the U.S. record industry joins the ranks of DRM mandate opponents); <http://alliancefordigitalprogress.org>.

²⁰⁷⁷ See: <http://www.freedom-to-tinker.com>. See also: Stallman (2002a): 115; and *supra* note 2066.

nologies.²⁰⁷⁸ It may impede competition between the old standardized DRM technology and newly emerging technologies and thereby hold up technological innovation.

VII Conclusion

This article started with two goals. Firstly, it attempted to show that, in the future, we might be confronted with new kinds of policy problems that are underrepresented in the current DRM debates. The tension between DRM and copyright law is only a small part of the overall DRM policy debate. The article highlighted several issues that stem from other areas of law and public policy, in particular from competition-related concerns.

Secondly, the article argued against fundamentalist viewpoints in the DRM policy debate. While the author shares many of the concerns raised against DRM, this article attempted to show that in many cases, DRM technology and its surrounding framework are much more flexible than commonly assumed. Unfortunately, over the last few years, the DRM debate has developed into a discussion about extremes. Depending on the point of view, digital rights management is perceived as either heaven or hell on earth. Some DRM opponents consider the potential threats of DRM as so dangerous that they condemn the idea of digital rights management altogether.²⁰⁷⁹ However, to argue that DRM will inevitably lead to an Orwellian world of perfect private control suffers from a general problem cyberlaw has to deal with: although a world of perfect control would indeed be highly undesirable, it is often unclear whether such perfection will ever occur in the real world.²⁰⁸⁰ Particularly in an area such as DRM, where technology seems capable to reflect many of the objections raised against the technology, unconditional opposition to the technology seems inappropriate at this time.

Naturally, framing the DRM debate as a debate about extremes has its own reasons. The most important reason may be that it is easier to talk about clear-cut extremes — DRM as paradise for creators versus DRM as hell for consumers — than to grapple with the muddy middle ground in between. However, debating about DRM in terms of extremes disguises the insight that such middle ground may exist and be preferable. The difficulties to conceptualize balanced DRM regimes as well as the staggering complexity of innovation policy in general should not deter technologists, lawyers, legal scholars, economists and policy makers from attempting to crystallize this middle ground.

Currently, no one knows whether a balanced DRM system that protects interests of users and the society at large is ultimately feasible both from a technological and a business perspective. The potentials of DRM to create a balanced and

²⁰⁷⁸ See: *Biddle, England, Peianado, Willmann* within this book: 356–357 (arguing against a statutory watermarking mandate due to various technical inadequacies of digital watermarks).

²⁰⁷⁹ For a general analysis of such slippery slope arguments, see: Volokh (2003).

²⁰⁸⁰ For the same argument in a different context, see: Bechtold (2002a): 242.

just information ecology are still largely unexplored. As all technology, DRM is malleable, and one should not miss the opportunity to engage in a value-centered design process that shapes DRM appropriately.

A Getting Insights: DRM Conferences 2000 and 2002

Eberhard Becker, Dirk Günnewig²⁰⁸¹

This Annex summarizes the proceedings and conclusions from the two DRM conferences that were held in November 2000 and January 2002 in Berlin.

Because of the various challenges and the several disciplines involved as described in the main part of this book, the two interdisciplinary conferences were organized in the context of the Research Alliance Data Security North Rhine-Westphalia. They aimed at approaching different DRM-related disciplines that had evolved in Germany, Europe and the United States. Especially US-based researchers were invited to help utilizing their current advanced experiences in the German and European context.

At the conferences, jurists and lawyers analyzed the legal challenges of the digitalization of content, and the application of DRM-systems for the protection of intellectual property (IP) embedded in such content; engineers gave lectures on technological challenges in the development of components for DRM systems, and DRM technology and DRM service providers demonstrated their approaches. Furthermore, lobbyists had the opportunity to express their views and goals with respect to the design and use of DRM systems and the use of content and IP in the digital age.

While the conferences had similar programme structures, the attendees were more technology oriented at the 2000 workshop than at the 2002 conference²⁰⁸³. This seems to indicate that the view that DRM is not just about technology had become more commonplace. Also obvious was that DRM had become more of a public issue: while the first meeting was attended by three journalists only, the second drew more than twenty to Berlin.²⁰⁸⁴

Both conferences were seeded by the Research Alliance Data Security North Rhine–Westphalia²⁰⁸⁵. The Alliance is an interdisciplinary association of scholars from mathematicians via engineers, computer scientists to legal and political scientists. It was founded in April 1999 to further applied research in the field of cryptography and security of information technology.

The two conferences were organized within the Alliance’s project “Management of digital goods — Schutz digitaler Güter” that was located at the Department for Mathematics at the University of Dortmund, and the European Institute for IT-Security at the Ruhr–University Bochum. The concepts for both conferences were developed by Prof. Dr. Eberhard Becker, Dr. Tomas Sander and Dirk Günnewig, Petra Henseler (2000) and Dr. Stefan Bechtold (2002).

²⁰⁸² Universität Dortmund.

²⁰⁸³ Some spoke about an “*invasion of jurists and lobbyists*” . . .

²⁰⁸⁴ Some of their reports are available on: <http://www.digital-rights-management.org>, unfortunately only in German.

²⁰⁸⁵ See: <http://www.datensicherheit.nrw.de>.

The following two Annexes (A.1 and A.2) summarise the discussions and results of two conferences while the conference web site²⁰⁸⁶ contains recordings of the some parts of the conferences (offered for download as MP3s — without DRM), short biographies of the speakers and many of their papers, abstracts and presentations. The following summary concentrates on main aspects discussed at the two conferences in Berlin. The topics of the lectures are dealt with in greater details in the articles of this book. This appendix aims at conveying the flavour of the lectures and the discussions of the two conferences. Finally, Annex A.3 supplies the programmes of the two conferences.

²⁰⁸⁶ <http://www.digital-rights-management.org>

2.6 Trusted Platforms, DRM, and Beyond

*Dirk Kuhlmann*⁴¹⁴, *Robert A. Gehring*⁴¹⁵

I Introduction

It is not immediately obvious why a book on Digital Rights Management should include a chapter about Trusted Computing, although a number of publications have investigated the suitability of trusted systems as rights management platform. Until recently, however, they have been of little more than remote interest for DRM as well as for typical business or consumer environments, as they were considered to be inflexible and cumbersome to manage.

This has changed dramatically with the advent of the technology developed by the Trusted Computing Platform Alliance (TCPA). Although this technology has primarily been propagated as security improvement of networked end systems, multiple observers were quick to point out that some basic features were similar to mechanisms that allow to support DRM. In some extreme cases, TCPA has literally been equated with DRM, this is, as a thinly veiled attempt to introduce ubiquitous control mechanisms on formerly open PC architectures.

As an introductory remark, it is sufficient to point out that the apparent contradiction between “openness” and “full user control” on the one hand and “closedness” or “constrained user behaviour” constitutes a similarity between requirements of DRM and system security. Consider computers in organisational and corporate environments: once a machine is part of a collaborative network and processes data that is subjected to external policies, full user control gives rise to a number of problems. It allows users to install and run arbitrary software for both corporate and private purposes. This can easily create security vulnerabilities, something network administrators are very aware of keen to prevent.

Copyright holders are facing a similar problem. Personal computers can include software media players to display digital content, but as the user has full control, they can also be used for storing, duplicating, and disseminating the content in ways not endorsed by copyright regulations. The proliferation of cheap and powerful multimedia PCs and the convergence of digital storing technology (e.g., compact disc) has created a situation where copyright owners have effectively lost control over digital copies of their works.

These and other dilemmas have renewed the interest in mandatory control mechanisms and trusted systems. These systems can enforce rules users have to adhere to when interacting with resources that have multiple stakeholders. In other words: the user can not override the policy while maintaining access to the resource subjected to this policy. This can significantly improve confidence in the expected behaviour of an IT system as it allows fine-grained control over what

⁴¹⁴ Hewlett Packard Laboratories, Bristol.

⁴¹⁵ Technische Universität Berlin.

computers and their users can do at any given time. TCPA and Trusted Platform technology claim to address the problem of how to gather and communicate indicators about what behaviour to expect.

This paper is an attempt to scrutinise arguments that concern TCPA's potential as DRM technology. We will start with an outline of TCPA (v. 1.1b) in terms of its context, basic features, and critique it has encountered, followed by an overview of trusted systems in general that discusses both the traditional concept of 'trust' in IT security and more recent attempts to apply this approach to digital rights management. This allows us to analyze commonalities and differences between traditional and DRM-focused trusted systems. We conclude with a discussion of the future of Trusted Platform technology and some thoughts on technology regulation.

II Trusted Computing Platforms

IT security vulnerabilities have become an increasing problem during the recent years. As of 2003, an average of 11 new bugs are reported every day⁴¹⁶, and this number is rising. As a consequence, security remains a major concern for both corporate and private IT users.

There are a number of factors that contribute to this situation. To name only three of them:

- Most users have little if any idea about what is going on behind their graphical user interface. Even administrators frequently do not have a comprehensive understanding about what is actually happening on their machines.
- All software can be tampered with before or while it is running. As a consequence, systems whose security relies on software alone ultimately can not vouch for their own status and integrity.
- Even if our current IT systems were more secure, they could not communicate this fact in a trustworthy manner to remote peers. Trust relationships between technical systems currently have to be established out of band by their owners.

The current lack of confidence the security of IT can at least partially be attributed to two major advantages of today's end systems and networks — namely, their openness and flexibility, which are often considered as fundamental values. However, one might argue that the extent to which a system should be flexible and open depends finds its natural limitations in the purpose it serves to its owner and his communicating peers at any given point in time. In some situations, maximum openness and flexibility are desirable. In others, the exact opposite might be true.

Systems that put emphasis on security rather than on versatility have traditionally been designed for environments where concerns of confidentiality, integrity and separation of roles are prevalent under almost all conditions, e.g. for the

⁴¹⁶ See: CERT (2003).

military and financial sector. They tend to be governed by rigid polices, and much research has been done to find suitable access control mechanisms, in particular for operating systems⁴¹⁷. Unfortunately, these designs tend to counteract the aforementioned advantages of openness and flexibility while simultaneously imposing a penalty of additional system management.

Trusted platform technology as discussed in the following sections claims to combine the advantages of both worlds. It starts from the understanding that in everyday situations, security is a flexible notion rather than an absolute goal: in order to be trustworthy, a system just has to be secure enough to be fit for purpose. Trusted platforms do not insist on provable security for all conditions – even less so since the user may not understand and therefore not trust the proof. It is deemed more important that a trusted party vouches for the fact that a particular system configuration and policy is fit for a particular purpose.

Apart from enforcing policies, Trusted Platforms address two other problems mentioned above. The design sets out to provide for a mechanism to reliably record the system state and to report it upon request. This allows to communicate state information from a local machine in a way that is trustworthy to a remote party.

II.1 The Trusted Computing Platform Alliance

The Trusted Platform Computing Alliance (TCPA) was created in 1999 by Compaq, HP, IBM, Intel, and Microsoft, all of which became members of the organization's steering committee. Since its creation, the TCPA has been joined by more than 170 other companies and organisations. Apart from the major platform and software companies just mentioned, the consortium includes, amongst others, chip and BIOS producers, vendors of authentication or security technology and services, and financial or content service providers.⁴¹⁸

Although the alliance started out with a PC specific agenda, TCPA design characteristics now cater for other a wide range of networked IT such as servers, network appliances, mobile phones, PDAs, and consumer electronics. This has broadened TCPA's appeal even further, and while this article is written (March 2003), the consortium is undergoing a major process of reorganisation that accommodates a wider and more diverse membership.

Since its formation, the alliance has created the current TCPA "Main Specification" 1.1b⁴¹⁹ and a PC-oriented "Implementation Specification"⁴²⁰. For the TCPA hardware component, the "Trusted Platform Module" (TPM), was defined, and its version 1.9.7⁴²¹ has since been certified by NIST according to the Common Criteria Evaluation Assurance Level EAL3+⁴²².

⁴¹⁷ Overviews can be found, e.g., in Pfleeger (1996); Anderson (2001); Bishop (2003).

⁴¹⁸ For details, see the TCPA membership list at:
<http://www.trustedcomputing.org/tcpaasp4/members.asp>.

⁴¹⁹ See: TCPA-Spec (2002).

⁴²⁰ See: TCPA-SpecImpl (2002).

⁴²¹ See: TCPA-TPMProf (2002).

II.2 TCPA — Motivation and Approach

The IT industry sees itself under increasing pressure from government, businesses and consumers to improve security aspects their products and services. So far, the success of respective efforts has been quite limited. This can partially be explained by the fact that neither the Internet protocols nor the PC have originally been engineered for the purposes they are used for today.

The common Internet Protocol (IP) ignored security aspects almost completely. The same is true for many transport, signalling, and management protocols that constitute the building blocks of today's infrastructure and have been built on top of IP. As a consequence, deployment of security enhanced systems becomes difficult as soon as contributing nodes are part of different organisational domains and subjected to different policies. This situation is increasingly typical for today's Internet: current practices of outsourcing, contracting and collaborative work make it desirable to allow access to precisely defined subsets of system resources, and there is an increasing need to support policies even across organisational and corporate levels.

PCs and their operating systems were originally designed for standalone purposes. Over the last two decades, they have been continuously extended to make them usable as network nodes. Workstations and other end systems now include features that would previously have been considered as elements of networked servers. This has made them more vulnerable to remote subversion and more suitable as tools or launching platforms for hostile attacks. This problem of end point security and trustworthiness is the one TCPA has set out to address.

Given that it was possible to create such a broad industry alliance to tackle end point security, one can safely assume the existence of major technical, economical and political drivers behind the agenda of trustworthy computing. Existing technical deficiencies and continued governmental pressure are likely to play an important role here. Apart from this, there are straightforward economic factors that may motivate support of TCPA's agenda. Depending on their respective commercial activities, consortium members could be motivated by the following considerations:

- TCPA requires an additional hardware component to be embedded on motherboards, which makes this technology interesting for chip producers.
- TCPA relies on security validation and certification, which makes it attractive for evaluation laboratories and PKI vendors.
- Lack of adequate security for end systems has been named as a major inhibitor for ubiquitous e-business and e-government, and e-service providers may see TCPA as enabling technology.
- Last, but not least, content providers and software vendors are likely to view TCPA as a promising technology to protect their rights on digital content⁴²³.

⁴²² See: NIST (2002).

⁴²³ Content protection is not copyright protection since the copyright laws do not acknowledge mere "material" and/or "metadata" as subject matter for copyright protection. The paradigmatic change hidden behind this chosen terminology ("content") is broadly discussed in: Bechtold (2002).

Given the extent of TCPA’s intended usage, security requirements will vary widely due to different usage contexts and platforms. To comprehensively cover this variety in a technical specification is close to impossible, which is likely to be the reason why TCPA steers makes minimal assumptions about usage scenarios. It assumes little more than that every platform has an owner. In addition, the specification reflects the common situation where users do not own the platforms they are working with.

One of TCPA’s most emphasised features is a set of mechanisms to reliably record and report the configuration and state of a platform. Since trustworthiness is a multilateral problem in the networked world, reliable reporting not only has to satisfy the local user of a machine, but also peers he is communicating with. Trusted platform technology provides a number of building blocks to address this problem.

There are two ways how users can convince themselves that a system is adequate for an intended action. They either base their decision on their own understanding of technology or they trust a third party that vouches for the system’s “fitness for purpose”. It should be emphasised that “fit for purpose” is a pragmatic notion and different from “secure”. Trusted platforms can support judgements about the level of risk that they might not behave as expected. Secure systems are designed with the goal to minimise or exclude risk. Clearly, secure systems can be built on top of Trusted Platform technology.

Systems that are built on top of TCPA technology can exploit its features to ensure the integrity of the system configuration once it has been accepted. This includes enforcement of any particular policy that is part of this configuration. How they do this is not defined by TCPA; Trusted Platforms technology as such is oblivious to any specific policy or configuration.

II.3 TCPA Technology and Infrastructure

The TCPA architecture consists of three principal elements: hardware, software, and infrastructure (see figure 1).

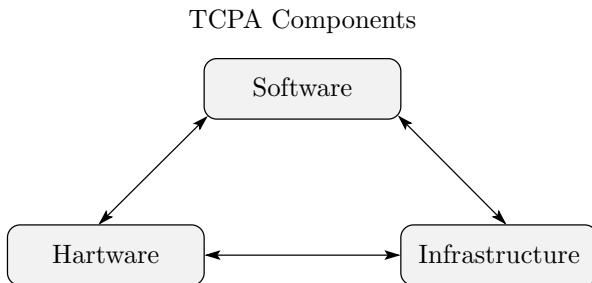


Fig. 1. TCPA Components⁴²⁴

The interaction between these components is quite complex and can only be outlined in this section. For a more comprehensive overview, the reader is referred to

⁴²⁴ Unless stated otherwise, all figures are © 2003 Robert A. Gehring.

Pearson⁴²⁵ and the specification proper⁴²⁶. A number of common misconceptions are addressed by TCPA⁴²⁷ and Safford⁴²⁸, and this article, respectively.

Hardware

The hardware component (Trusted Platform Module or TPM) provides functionality that is roughly equivalent to that of a state of the art smartcard. It includes a random number generator, a generator for RSA key pairs, and a limited amount of non-volatile storage. The non-volatile memory on the chip is considered shielded: at the level of the chip's tamper-resistance, it is protected from interference and prying.

Some of the non-volatile memory on the TPM is used to store two 2048 bit asymmetric key pairs. One of these key pairs, the Endorsement key, is generated at the vendor's premises during production time and is the single unique identifier for the chip. The second pair, the Storage Root Key, is generated when a customer takes ownership of the TPM.

During the process of taking ownership, the prospective owner defines an authorization secret that he has to provide to the TPM from then on to enable it. The private parts of both the Endorsement and the Storage Root keys are stored exclusively inside the TPM. The owner can not use the private part of endorsement key to sign or encrypt data. In order to decrypt data that has been encoded using the public part of the endorsement key, knowledge of the authorization secret is required.

The remainder of the non-volatile memory on the TPM is organised as two sets of registers. A Platform Configuration Register (PCR) is designed to store values that represent the complete history of its modifications; a Data Integrity Register (DIR) has the same size as a PCR. It can hold an arbitrary value of up to 160 bit length that typically reflects the expected value of a corresponding PCR.

Most TPM commands are essentially combinations of the basic functions mentioned above: authorization secret, key protection, key generation, shielded configuration registers and integrity registers. Amongst others, the TPM supports to:

- employing asymmetric key pairs that can not be used by software, but only by a TPM,
- logging system events in a non-reversible manner, supporting reliable auditing of the system's bootup and configuration,
- binding the capability to decrypt data to a specific platform state

Most operations are not provided by the TPM on its own, but need operating system and application software support.

⁴²⁵ See: Pearson, Balacheff, Chen, Plaquin, Proudler (2003).

⁴²⁶ See: TCPA-Spec (2002).

⁴²⁷ See: TCPA-QA (2002).

⁴²⁸ See: Safford (2002a).

Software Support

TCPA compliant end user systems require two types of software. The first type, the Trusted platform Support Service (TSS), implements a number of complex functions that need multiple invocations of the TPM and symmetric encryption functionality. The second type, called “Core Root of Trust for Measurement” (CRTM), is part of the platform firmware. It will typically reside in a BIOS or chipset and executed at an early stage of the platform bootup. Its task is to generate hash values of all binary code that is about to be executed and to log these values into the PCRs of the Trusted Platform Modules.

The core idea is to extend this type of “software measurement” from the firmware and the BIOS to the operating system (OS), OS services and applications. TCPA defines the chain of integrity verification up to the OS boot loader. Specific boot loaders or operating systems are not covered by the specification. As of the current specification, TCPA is OS-neutral.

Infrastructure

TCPA based systems include indicators that help to determine the level of confidence users can have in a given software environment. This judgement can be based on trusted statements of other parties. In order to communicate these statements, TCPA needs support of digital signatures, certificates, and public key infrastructures.

The first certificate concerns the unique identifier inside the TPM, the endorsement key. It attests that the private endorsement key resides on a TPM of a specific type, on this TPM alone and that it has never been disclosed to anyone.

The second certificate attests that a specific TPM with a specific endorsement key has been properly integrated on a motherboard of a specific type.

Platform credentials include a reference to a third kind of credential, the conformance certificate. It vouches for the fact that the combination of a TPM and a specified type of motherboard meet the TCPA specification, e.g., because both meet the Protection Profiles mentioned in section II: *The Trusted Computing Platform Alliance* on page 180.

The last certificate type can combine all aforementioned credentials in a single statement. The TCPA specifications envisages these “identity certificates” to be issued as identifiers for Trusted Platforms. It is noteworthy that:

- identity certificates do not need to reflect attributes of human users in any way, as they identify platforms;
- a single Trusted Platform can have an arbitrary number of identity certificates, hence multiple identities;
- requests for identity certificates do not require to prove platform ownership to a remote party.

Figure 2 shows the composition of TCPA components and their infrastructural dependence on Certification Authorities⁴²⁹.

⁴²⁹ See: TCPA-TPMProf (2002); Pearson et al. (2003).

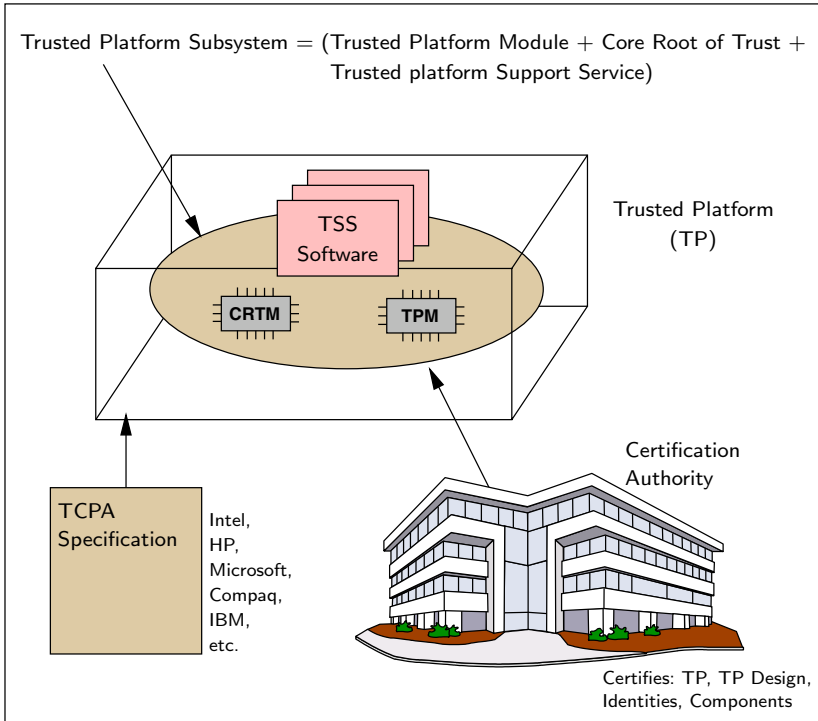


Fig. 2. Composition of TPCA Components⁴³⁰

Certification Authorities (CAs) that issue TPCA identity certificates may follow arbitrary policies since the specification is agnostic about particular CA policies and platform configurations. CAs may require a specific protection level attested as by the conformance certificate.

In principle, all TPCA mechanisms can be used without involving *external* certificate authorities. Platform owners, be it organisations or individuals, can issue identity certificates for themselves.

II.4 Critical Reactions

The concept of “Trusted Computing Platforms” as proposed by TPCA has drawn heavy criticism from security experts, computer scientists and consumer protection organisations even before its deployment.

An impartial observer will, at least in part, blame the TPCA itself for the criticism: The development process of the TPCA specification was not open to contributions or comments from the public and statements of some TPCA members regarding their intentions to deploy the technology raised suspicion of hidden actions and intentions.

⁴³⁰ Source: Pearson et al. (2003): 7.

This section gives a cursory overview of the main arguments of the critique. They can not all be scrutinised for their merits here. However, the most common point, namely, the equation of TCPA with DRM, deserves an in-depth exploration. This will be done in section III of this paper.

The objections⁴³¹ against TCPA can be roughly categorised as follows:

TCPA Means DRM

A number of critics maintain that the main purpose of TCPA is to embed hardware support for Digital Rights and Software management on end user platforms. They question the motives and intentions of the TCPA consortium and, in particular, the large corporations that constitute the steering committee, on principal grounds.

TCPA Means Less Freedom

Critics have pointed out the potential for misusing TCPA technology, e.g. for censorship and customer lock-in. The warnings that TCPA could put restraints on free speech are derived from the same warnings directed against DRM technology.

From a consumer protection point of view, it is claimed that TCPA solves the providers' rather than the users' problem. By supporting to constrain what users can or cannot do with their computers, more consumer value could be destroyed than is created by better trustworthiness.

TCPA Means Less Privacy

Since TCPA is widely equated with DRM, reproaches for undermining privacy directed against DRM technologies are regularly applied to TCPA too. The most important reproach refers to the impossibility of consuming media content in privacy due to the built-in feature of many available DRM systems to collect media usage information and to transfer it to content owners.

TCPA Means Less Security

It has been claimed that TCPA based technology could make reverse-engineering of DRM and security components harder. In conjunction with legal prosecution of reverse-engineering, this may lead to a situation of less rather than more trustworthiness.

TCPA Means Less Competition

Concerns have been raised with respect to potential negative consequences of TCPA in economical, social or political terms. Without objecting to TCPA as such, these critics argue that this technology will inherently cement current quasi-monopolies in the hardware and software sector and may create new ones in the content industry.

⁴³¹ More detailed criticism can be found, e.g., in: Anderson (2003); Arbaugh (2002); Green (2002); Cryptography (2002); Cypherpunks (2002) (from June 22, 2002 onwards).

TCPA Means More Security-Relevant Problems

A number of issues have been named that are linked to TCPA's hardware- and infrastructure based approach. They concern e.g. problems of (a) proving the trustworthiness of the on-chip random number and RSA key generators; (b) consequences for virtualisation layers and emulators; (c) potential large-scale abuse of the mechanism by bogus endorsement and identity certificates dissemination or revocation.

Summary

To wrap up: TCPA critics object the technology on the grounds that Trusted Platforms mean DRM, less competition,⁴³² less freedom — including less freedom of choice, and less control⁴³³ Supporters of TCPA have upheld that much of the critique is based on speculation and limited understanding of the technology, and that mutual assurance for IT systems is a real and pressing issue that is independent of any given political and economic context and has to be addressed where it crops up: at the level of technology.⁴³⁴

A cautionary observer may conclude that both critique and rebuttals are dissatisfying and that further discussion is in place.

III Trusted Systems vs. DRM Systems — Deblurring the Lines

That TCPA should be considered as some kind of DRM is a key part of almost every critical statement about the concept.⁴³⁵ The reasons for this assumption can be traced back to different motives, some obscure ones and some meritorious ones. We find technical arguments mangled with conspiracy theories and ample speculation based on misunderstandings. To make a serious judgement on these issues, we first have to deblur the lines between the concepts of trusted systems, trusted computing platforms, and DRM systems. We focus here on trusted systems and trusted computing platforms because DRM systems are exhaustively treated in this book.

For reasons of historical developments, we start with a portrayal of trusted systems.

⁴³² Most recently Anderson (2003a).

⁴³³ According to prominent critic Ross Anderson, they are probably even less secure, because a “trusted system or component” is defined as “one which can break the security policy”, implying that a “trusted computer” is one “that can break my security” Following this line of logic, the only computer where our security can not be broken is an untrusted one (since no one would expect security in first place). See: Anderson (2003): par. 24, 25.

⁴³⁴ More detailed answers to the critics can be found, e.g., in: TCPA-QA (2002); Safford (2002a).

⁴³⁵ See, e.g.: Anderson (2003); Yodaiken (2002); Weber (2003); Grassmuck (2002).

III.1 The Classic Approach to Trusted Systems

Trusted systems are neither new nor invented by the TCPA. Actually, research on trusted systems dates back to the 1960s and was driven by government and military needs for effective protection of information. The development of the Trusted Computer System Evaluation Criteria (TCSEC) from 1983 to 1999, also known as the Orange Book, was the first culmination of those research activities. Since its development was driven by governmental institutions, confidentiality is the main focus of the TCSEC. Data integrity and system availability, usually goals of information security,⁴³⁶ are of less importance within the TCSEC framework⁴³⁷.

Two research approaches were particularly influential on the formulation of the classic concept of trusted systems:

- The reference monitor concept introduced in 1973 by James Anderson;⁴³⁸ and
- The Bell–LaPadula (BLP) model as introduced in the same year by D. Elliott Bell and Leonard J. LaPadula.⁴³⁹

BLP was developed for a military environment, Anderson’s reference monitor has been conceived as a proposal for governmental establishments. BLP is a *policy model*, describing a specific way of controlling access to system resources. It is primarily concerned with restricting the information flow between formally distinguished security levels and compartments. The reference monitor concept, on the other hand, models a *system architecture* suitable to enforce policies. The monitor can be regarded as container to be filled with a rule set of choice (which could follow the BLP model as well as completely different ones). This concept is more generic, as it allows to employ arbitrary policies that might be better suited to meet modern business requirements for sharing information than the rather restrictive BLP.

The following short discussion may help to understand some peculiarities of the TCPA approach to evolve ordinary computers into trusted computing platforms. We start with pointing out some basics of the reference monitor concept.

The Reference Monitor Concept

According to Bishop⁴⁴⁰, “a reference monitor is an access control concept of an abstract machine that mediates all accesses to objects by subjects.” Figure 3 shows the schematic structure of the reference monitor concept⁴⁴¹.

Conceptually speaking, a reference monitor is nothing more than a container for a security policy. If we “fill” this container with a certain security policy, i.e. with defined subjects, objects and relations between them (e.g., security clearances

⁴³⁶ See, e.g.: Pipkin (2000): 14; Stallings (1999): 5).

⁴³⁷ See: Bishop (2003): 574.

⁴³⁸ See: Anderson (2001): 140.

⁴³⁹ See: Anderson, Stajano, Lee (2001): 189.

⁴⁴⁰ See: Bishop (2003): 502.

⁴⁴¹ See: Stallings (1999): 530.

and classifications), it will enforce the policy (what is allowed, what is forbidden) circumscribed thereby.

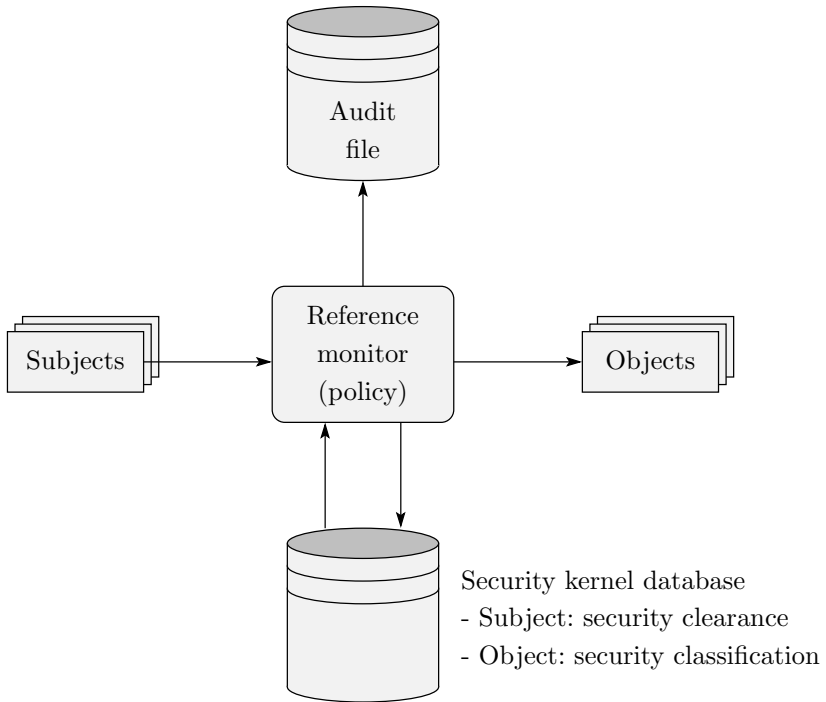


Fig. 3. The Reference Monitor Concept⁴⁴²

The implementation of a reference monitor concept is called a “reference validation mechanism” (RVM) and shows the following properties⁴⁴³: (1) It is tamper resistant;⁴⁴⁴ (2) it cannot be bypassed; (3) it is small enough for complete validation⁴⁴⁵. Around the RVM, the “trusted computing base” (TCB) is built. “A *trusted computing base (TCB) consists of all protection mechanisms within a computer system — including hardware, firmware, and software — that are responsible for enforcing a security policy.*”⁴⁴⁶

⁴⁴² Source: Stallings (1999): 530.

⁴⁴³ See: Bishop (2003): 502.

⁴⁴⁴ In fact, Bishop uses the term “tamper proof” here. For some critical analysis of so-called “tamper proof” devices, see: Anderson, Kuhn (1996/1997); Bao, Deng, Han, Jeng, Narasimhalu, Ngair (1997).

⁴⁴⁵ In practice, however, the third criterion quite often cannot be fulfilled due to “size or complexity of the reference validation mechanism”, as the Orange Book acknowledges. Nevertheless, we speak of a TCB in such cases too. Cf.

<http://www.kernel.org/pub/linux/libs/security/Orange-Linux/refs/Orange/OrangeI-II-6.html>.

⁴⁴⁶ See: Bishop (2003): 502.

According to the TCSEC (“Orange Book”), “[t]he heart of a trusted computer system is the Trusted Computing Base (TCB) which contains all of the elements of the system responsible for supporting the security policy and supporting the isolation of objects (code and data) on which the protection is based.”⁴⁴⁷

Trusted systems are built upon a TCB. According to Stallings⁴⁴⁸, a trusted system then is “[a] computer and operating system that can be verified to implement a given security policy.”

One property of the trusted system concept that might not spring to mind at first glance is its policy–neutrality.⁴⁴⁹ You can imagine almost any security policy⁴⁵⁰ that is enforced by the reference monitor as conceptualised above. Those who draft the policy and craft the code to enforce it are the ones who put the values into the system. The system will behave according to the values represented as policy and code.⁴⁵¹ This approach, however, is rather static. Typically, hardware, software, and policy as a whole are evaluated against defined criteria. A certificate attests compliance with these criteria for the system as a whole. Changing security relevant components on the fly invalidates the attestation, which means lack of flexibility to adapt to new (security) needs and goals. While being appropriate for environments with constant structures and tasks, this makes less sense for newly emerging technologies and services. With regard to new business models in a networked world, a different approach to trusted systems has been put forward by Xerox scientist Mark Stefik.

III.2 Trusted Systems According to *Stefik*

In an influential article,⁴⁵² Mark Stefik⁴⁵³ has given a new coat of paint to the old concept of trusted systems.

⁴⁴⁷ Cf. Orange Book, loc. cit.

⁴⁴⁸ See: Stallings (1999): 543.

⁴⁴⁹ But note that the policy–neutrality, while given in theory, may not be implemented in practice. Actually, due to issues of complexity and validation, most concrete trusted systems are not policy–neutral.

⁴⁵⁰ See: Schneider (2000): 30 f., defining a “security policy” as follows:

“A security policy defines execution that, for one reason or another, has been deemed unacceptable. For example, a security policy might concern access control, and restrict what operations principals can perform on objects; information flow, and restrict what principals can infer about objects from observing system behaviour; availability, and restrict principals from denying others the use of a resource.”

⁴⁵¹ Below the digital surface, the combination of digital numbers “structures and constrains social and legal power”. Moreover, we can think of code as a significant part of the institutions of the emerging information society. In the words of Douglass North (1999: 495), “Institutions are the rules of the game — both formal rules and informal constraints (conventions, norm of behaviour, and self-imposed codes of conduct) — and their enforcement characteristics.”

⁴⁵² See: Stefik (1997).

⁴⁵³ Mark Stefik was perhaps not the inventor of this “reevaluation of all values” (Nietzsche) but surely its most influential proponent. Lawrence Lessig, e.g., in his

The intention of his verbal take-over was to transform a standard computer technology into a “copyright box”⁴⁵⁴. And so he describes the new understanding for trusted systems:

*“A trusted system is a system that can be relied on to follow certain rules. In the context of digital works, a trusted system follows rules governing the terms, conditions and fees for using digital works.”*⁴⁵⁵

Stefik pursued his approach further and discusses trusted systems in the context of the Internet as:

*“systems, which protect digital works using a set of rules describing fees, terms, and conditions of use. These rules, written in a machine-interpretable digital-rights language, are designed to ensure against un-sanctioned access and copying and to produce accurate accounting and reporting data for billing.”*⁴⁵⁶

A quite simple concept designed to enforce, in principle, freely selectable security policies is thereby transformed into a concept for the enforcement of “digital rights” — “machine-governed rules of use” for content such as “[c]reative works.”⁴⁵⁷

If we try to precisely identify all the parts of Stefik’s approach to trusted systems, we can list them as follows: (a) access restriction; (b) copy restriction; (c) use control; (d) accounting; (e) reporting for billing.

In analogy to figure 3 showing the reference monitor concept, we can sketch Stefik’s design as shown in figure 4.

Two additional databases (dashed boxes) complement the database and audit file used by the reference monitor (renamed to DRM monitor for the sake of explanation). One database is needed to store the digital rights⁴⁵⁸ and one for the accounting and billing data generated during the subject’s use of protected objects.

To prevent any manipulation by the user, neither of the additional databases will be stored on the user’s system. Since the DRM monitor is at least in part managed by a source outside of the system’s boundaries, the objects are not under full control of the subjects anymore.

From the user’s point of view, the crucial issue is the concurrent implementation of two different access control mechanisms: one as described in the digital rights database and one as described in the security kernel database. According to

book “Code and Other Laws of Cyberspace”, quotes well known cryptographer Ralph Merkle with a Stefik-like statement (1999: 127). Nevertheless, many commentators consider Mark Stefik being the inventor of “trusted systems”. Cf., e.g., Griffith (1999) and Gimbel (1998).

⁴⁵⁴ See: Stefik (1999): 55.

⁴⁵⁵ See: Stefik (1997): Sect. II (A) Para. 1.

⁴⁵⁶ See: Stefik (1999): 55.

⁴⁵⁷ *ibid.*

⁴⁵⁸ For the sake of simplicity, we assume the implementation of the digital rights storage as a database. In practice, the necessary information is stored in part in a database and in part tied to the objects (e.g. as digital watermarks).

Stefik and other proponents of DRM systems, the thereby enforced DRM policy will have higher priority than the security policy under the user's control.⁴⁵⁹

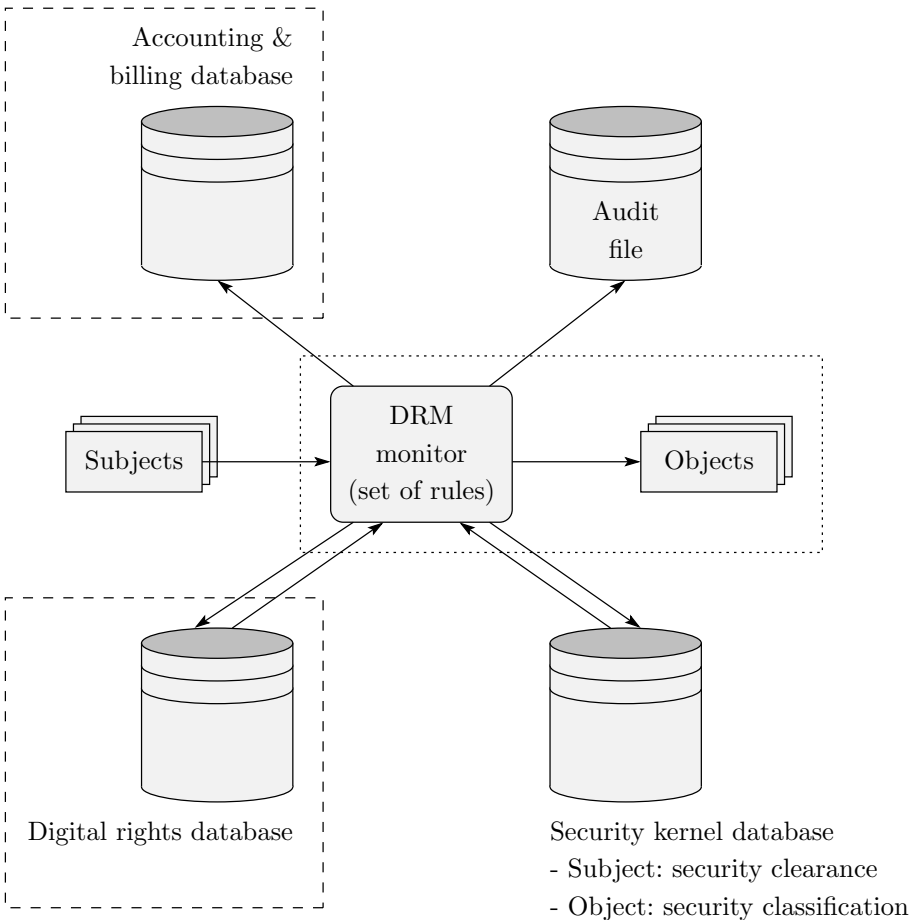


Fig. 4. Stefik's Design for Trusted Systems⁴⁶⁰

The main difference between trusted systems designed according to the classic concept and Stefik's trusted system is that the first ones are conceptually policy-neutral while the last one is clearly policy-specific.

Many people express their disagreement with these DRM systems by spelling them as "Digital Restrictions Management". As long as definitions of policies addressing digital rights are not in line with copyright law as well as with reasonable user expectations regarding freedom of speech, and protection of privacy,

⁴⁵⁹ This is exactly the meaning of the laws giving legal backing to such "trusted systems". Recent heavily disputed legislation — the Digital Millennium Copyright Act (DMCA) in the U.S., and the EU Directive 2001/29/EC in Europe — pinpoint the principle of primacy for digital rights management systems.

⁴⁶⁰ Figure based on Stallings (1999): 530.

criticism of systems built to enforce DRM will remain widespread. Nevertheless: simplistically applying the same criticism to the Trusted Computing Architecture means to overshoot the target.

III.3 From Trusted Systems to the Trusted Computing Platform Architecture

The description of trusted systems given above made a clear distinction between their (conceptually) policy-neutral and their (conceptually) policy bound appearance. How do Trusted Computing Platforms fit into this picture?

Compared to Stallings (see section II: *The classic approach to trusted systems* on page 188), Bishop⁴⁶¹ defines trusted systems from a more practical standpoint:

“A trusted system is a system that has been shown to meet well-defined requirements under an evaluation by a credible body of experts who are certified to assign trust ratings to evaluated products and systems.”

Certified authorities apply existing metrics (evaluation criteria) to an existing system (a constellation of hardware and software) in This yields a “*measure of trustworthiness, relying on the evidence provided*”⁴⁶². Since it is practically infeasible to create perfectly secure systems⁴⁶³, this measure has no absolute meaning, but reflects the relative level of faith or belief one can put in it. In the real and imperfect world, we therefore talk in terms of trust rather than those of security when making judgements systems based on this measure.⁴⁶⁴

It has already been mentioned that this approach is quite static. Changing requirements and/or modification of the system configuration that affect its security property may invalidate the assurances established in a previous evaluation process and can make it necessary to re-certify the system.

Today’s systems tend to be highly dynamic. New attributes can be added on the fly. Many of them are capable to interact: mobile phone with laser printers and cameras with computers. The requirement to continuously monitor, “measure”, and signal “fitness for purpose” (see section II: *TCPA — Motivation and approach* on page 181) goes beyond what the traditional trusted systems approach had to offer and has motivated the Trusted Platform concept.

Trusted Platforms come with small, embedded hardware elements delivering low-level functionality to the operating system and applications. Once initialised, the behaviour of these elements can not be changed other than by full reset: they can be relied upon behaving as specified. Using a very simple layer model, the architecture can be sketched as shown in figure 5.⁴⁶⁵

⁴⁶¹ See: Bishop (2003): 479.

⁴⁶² See: Bishop (2003): 478.

⁴⁶³ See, e.g.: Bishop (2003): 477.

⁴⁶⁴ There are many definitions of trust and trustworthiness and not all are consistent, whereby discussions about this topic are easily mislead. For a short description of the problem see: Anderson (2001): 9 f. The overloading of the word “trust” is confusing even for experts; some scientists argue that it will do more harm than good when applied to computer systems and transactions. For a discussion see, e.g.: Nissenbaum (1999); Friedman, Kahn, Howe (2000).

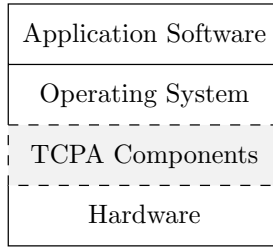


Fig. 5. A Layer Model for TCPA

The TCPA components (hardware and software) are inserted between the standard hardware and the operating system, and activated by “opt-in”.⁴⁶⁶ Taken on their own, the TCPA components do not provide more than a number of “bricks” to build a trusted computing platform⁴⁶⁷ from a conventional computer. The “mortar” comes from outside, from trusted third parties (TTPs⁴⁶⁸) that declare the trustworthiness of the “bricks”. To reflect this dependence on different stages from TTPs we enhance the above layer model. (The use of an index x for TTPs indicates the dependence from different TTPs.⁴⁶⁹)

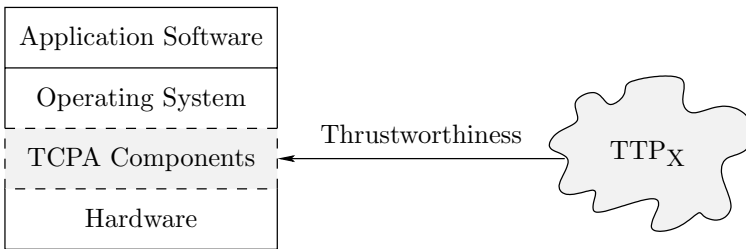


Fig. 6. TCPA Layer Model with TTPs

The layers above the TCPA layer, i.e. operating system and application software, can make use of the functionality provided in order to operate in a “trustworthy” manner. How far this goes depends on both operating system and application software. Relying on the TCPA components means: an access control policy will be enforced without unexpected interference — as long as the declaration of trustworthiness for the TCPA components holds.⁴⁷⁰ Thus, step by step, a trusted system configuration can be build up without the need to certification of the system as a whole. Compared to the classic approach to trusted systems, the trusted computing platform architecture provides much more flexibility.

⁴⁶⁵ One of the earliest descriptions of a TCPA-like architecture, the article by Arbaugh, Farber, Smith (1997), also argues along a layered approach.

⁴⁶⁶ In practice however, the borders are blurred.

⁴⁶⁷ See: Pearson, Balacheff, Chen, Plaquin, Proudler (2003): 44.

⁴⁶⁸ The trusted third parties (TTPs) are called “certification authorities” (CAs) in the TCPA terminology. See: Pearson et al. (2003): 298.

⁴⁶⁹ See *Infrastructure* in section II on page 184.

⁴⁷⁰ Due to lack of experience, it is hard to judge if this approach is feasible on a large scale.

The integration of TCPA functionality into the operating system and/or the application software requires the use of additional TTP support in order to retain the trust model. Again, certification of trustworthiness is provided by the TTP. A multi-user operating system, for example, could make use of certified identities. The integrity of system components will be certified accordingly. The actual level of trust is then derived from the level of trust before the integration of the new system component and its certificate, as shown in the next figure.

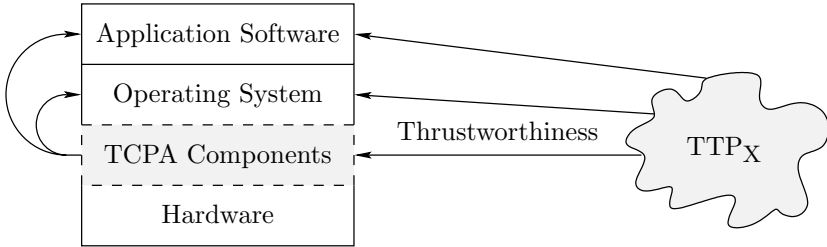


Fig. 7. Promoting Trustworthiness

Thus, trust is propagated through composition of the knowledge of an existing system configuration and authorised statements about new components. In the TCPA terminology, a “chain of trust”⁴⁷¹ is build.

In order to enable “trustworthy interaction” with other systems, the actual state of the system can be signaled to other systems. This is called “remote attestation”⁴⁷².

By evaluating this state, the remote system can decide whether the level of trustworthiness signaled by the local system is consistent with its own security policy. If the remote system decides to accept the level of trust signaled by the local system, for example, transactions initiated by the local system can take place.

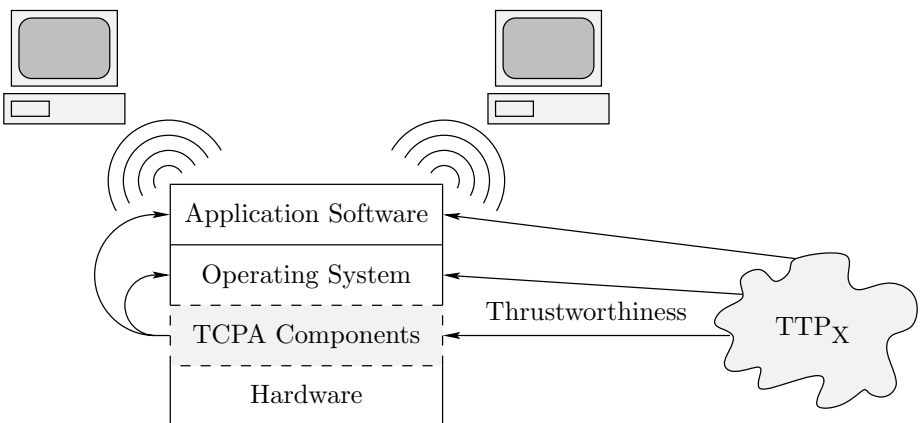


Fig. 8. Remote Attestation

⁴⁷¹ See: Pearson et al. (2003): 75.

⁴⁷² See: Pearson et al. (2003): 49.

TCPA provides “a special wrapping process that permits the caller to state the software environment that must exist in the platform before the TPM will unwrap a secret.”⁴⁷³

“Taken together, [enhanced protection of secrets and enhanced signatures] improve confidence for the owner of data that resides on remote computer systems. It becomes possible to store data on a remote computer and restrict the conditions under which that data can be used.”⁴⁷⁴

A wealth of possibilities to handle information according to different security policies is enabled by this TCPA functionality.⁴⁷⁵ There can be no doubt that DRM is one of the possibilities.

Although Pearson et. al do not explicitly refer to DRM, they write of “digital content delivery”⁴⁷⁶. “Digital content delivery” plus “restrict the conditions under which that data can be used” is a description of what DRM does. To put it bluntly, although TCPA does not define a DRM system, “trustworthy” DRM systems can be built using the TCPA components.

And here we can draw the line between DRM technology and TCPA technology. DRM technology, by definition, is policy-specific, built “to police copyright”⁴⁷⁷, while TCPA technology is conceptually policy-neutral, as was the classical concept of trusted systems before. At least from a strictly technological point of view, this statement holds.

Both proponents and opponents of DRM technology should realise this difference. When discussing the pros and cons of TCPA technology, or *whether* and *how* to regulate the deployment of this technology, the focus has presumably to be directed towards the other elements of the whole communication infrastructure: hardware, operating system, application software levels (local and remote), and certification services.

III.4 A Short Comparison of DRM and TCPA

Digital Rights Management (DRM) systems can be understood as follows:

*“Digital Rights Management (DRM) technology has emerged to protect and manage the commerce, intellectual property ownership, and confidentiality rights of digital content creators and owners as content travels through the value chain from creator to distributor to consumer, and from consumer to other consumers. In an enterprise environment, DRM is related to policy management, which controls access and management of information based on policies.”*⁴⁷⁸

⁴⁷³ See: Pearson et al. (2003): 46.

⁴⁷⁴ See: *ibid*: 47.

⁴⁷⁵ For an overview see: Pearson et al. (2003): 48–56.

⁴⁷⁶ See: Pearson et al. (2003): 7, 44.

⁴⁷⁷ See: Chris Hoofnagle in: Gaither (2002).

⁴⁷⁸ See: Duhl, Kevorkian (2001).

Based on the above made explications on the concept of trusted systems and the peculiarities of the TCPA approach, the following comparison between DRM and TCPA technology can be made:

<i>Criterion</i>	<i>DRM</i>	<i>TCPA</i>
<i>Relation to DRM</i>	is DRM	enables DRM (1)
<i>Direction</i>	“content”-centristic	“resource”-directed
<i>Policy</i>	policy-specific (enforce “digital rights” policies)	policy-neutral (enforce any access control policy)
<i>Legal status</i> (protection against circumvention)	protected by copyright laws (DMCA, Directive 2001/29/EC)	not specially protected (2)
<i>Optional</i>	(increasingly) no choice for “opt-in” or “opt-out”	specified as “opt-in” technology
<i>Hardware switch</i>	no hardware-based switch-off	hardware-based switch-off specified
<i>Standardisation</i>	different systems from different vendors (3)	standardised technology
<i>Privacy</i>	undermines users’ privacy (4)	can be used to undermine as well as to protect users’ privacy
<i>Security</i>	insecure (5)	(probably) hard to break
<i>Availability</i>	different systems available	almost ready for market (6)

Remarks

(1) DRM is one technology, and only one, that can be based on the components provided by TCPA.

(2) Since TCPA alone — as it is specified — is not capable of functioning as a “Copyright Protection and Management System” (as described in the DMCA), only *TCPA-derived technology* intended to be used as a DRM system is protected by copyright law against circumvention etc. Otherwise, by specifying a switchable “opt-in” solution, TCPA would possibly offend against the DMCA rules. Every switch disabling TCPA functionality had to be interpreted as “circumvent[ing] a technological measure that effectively controls access to a work protected under this title.”⁴⁷⁹ Additionally, TCPA will control access to computer resources that by no means, not even under the indistinct declarations of the DMCA, qualify for copyright protection.

(3) See also the article from *Chang* and *Rambhia* (discussing DRM and standardisation) in the present book on page 162.

(4) To protect users’ privacy is usually not a design goal for DRM developers, what draws continuing critique.⁴⁸⁰ Even the EU Commission, while pushing development and deployment of DRM systems, raises concerns that “[f]rom the individual’s perspective, the unlawful collection and processing of personal data

⁴⁷⁹ Title 17, United States Code, Chapter 12, §1201 (a)(1)(A).

⁴⁸⁰ See, e.g.: Cohen (2003/a).

for customer profiling and other uses by a DRM provider would constitute a threat to their privacy and could affect the willingness of consumers to accept DRMs.”⁴⁸¹.

(5) As different studies have shown, contemporary DRM systems provide only a medium level of security and, in fact, many systems do not even resist unsophisticated attacks.⁴⁸²

(6) IBM is already delivering some of its notebooks with a security chip and according software support. This *proprietary solution*, however, is not to be confused with TCPA. Nevertheless, it can be considered as some kind of a prototype of a trusted computing platform according to the TCPA specification.

IV The Future of TCPA

An updated version of the TCPA specification is currently under development. It can be expected to address well-known shortcomings of the current specification such as the simplistic audit mechanism⁴⁸³. As for the alliance itself, it has become obsolete after the formation of its successor, the Trusted Computing Group (see below).

TCPA has met a fair amount of criticism. Much of it, such as the notion of “TCPA-certified” operating systems and software, is based on misconception or mere speculation and has been dismissed as such by parties with vested interests⁴⁸⁴, but also by apparently independent analysis⁴⁸⁵. Other arguments, however, require careful consideration, not least because successful deployment of TCPA technology will critically rely on customer acceptance.

Many debates were actually centred around potential implications of “Palladium” — this is the old label for Microsoft’s efforts to build its own trusted platform (the name “Palladium” has since been replaced by the slightly more cumbersome one of “Next Generation Secure Computing Base” or NGSCB).

In the following, we give a brief overview of the Palladium / NGSCB approach and the hardware that underpins this architecture: Intel’s LaGrande technology. We will close this sections with some considerations about TCPA and Open Source and a first glimpse at the freshly founded Trusted Computing Group.

IV.1 TCPA and Microsoft’s Palladium / NGSCB

Although TCPA and NGSCB share some basic features, e.g. the TPM, Microsoft has made it clear that both have fundamentally different architectures.⁴⁸⁶

⁴⁸¹ See: EU-COM (2002): 14.

⁴⁸² See, e.g.: TÜViT (2002); EU-COM (2002); Pfitzmann, Sieber (2002).

⁴⁸³ See: Pearson et al. (2003): 71.

⁴⁸⁴ See: Safford (2002a): TCPA-QA (2002).

⁴⁸⁵ See: Anonymous (2002).

⁴⁸⁶ The following discussion is based on Microsoft’s Technical FAQ for the Next Generation Secure Computing Base. See: Microsoft Corp. (2003).

NGSCB's scope is much broader and it requires hardware support that goes far beyond what TCPA has to offer. such as those of Intel's LaGrande architecture (see below), as Intel security architect David Grawrock admitted⁴⁸⁷.

Palladium relies on a hardware component called "Security Support Component" (SSC), which has features that are very close, but not quite identical, to those offered by the TPM of TCPA. As of writing of this article (March 2003), it is still unclear whether the additional functionality required by the SSC (symmetric AES encryption) might be offered by a future version of TCPA, the chipset, the CPU, the BIOS, a combination thereof, or by a completely separate component. NGSCB creates a new environment that runs alongside the OS, the so-called "nexus". In combination with the CPU this component allows to "wall off" and hide parts of the memory from other applications and the operating system as shown in figure 9.⁴⁸⁸

According to Microsoft's FAQ, anyone can write a nexus for a nexus-aware system, users will be in control of what nexus runs on their machines, and dual-boot will be possible in the future. It is less clear, however, whether Microsoft's operating systems and nexus-aware applications will run with an arbitrary nexus, whether emulators and virtualisation layers will be affected, whether applications will employ persistent storage shielded by a particular nexus, and how attestation of applications will be obtained.

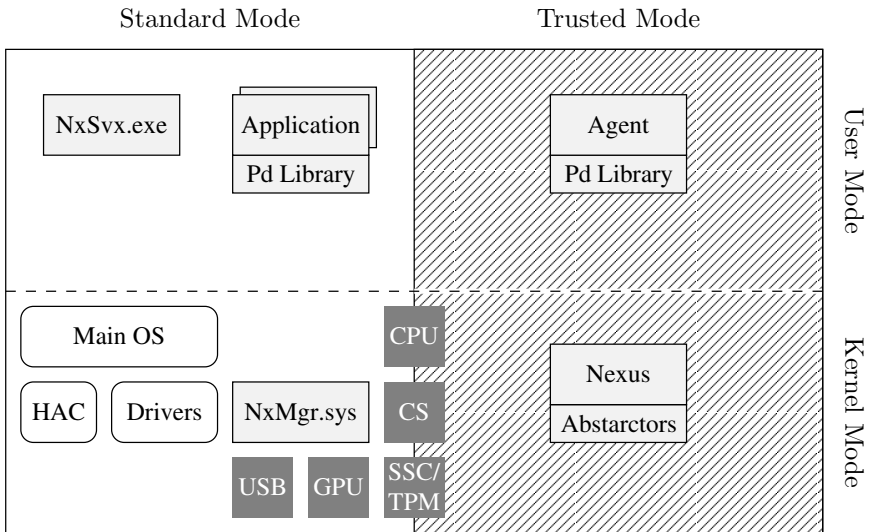


Fig. 9. MS Palladium/NGSCB Structure⁴⁸⁹

⁴⁸⁷ See: Plura (2003).

⁴⁸⁸ This figure shows the Palladium components before the concept was renamed to Next Generation Secure Computing Base. It is drawn after a picture shown in Himmelein (2003): 88.

⁴⁸⁹ Source: Microsoft.

Considered that TCPA has carefully avoided to include mechanisms for symmetric bulk encryption into the Trusted Platform Module (TPM) in order to avoid issues of export restriction, it seems quite astonishing that the SSC should contain such a capability in the first place.

IV.2 TCPA and Intel's LaGrande Processor Architecture

As of March 2003, Intel has disclosed very little information about its LaGrande architecture other than it will be released during the second half of the year⁴⁹⁰. Microsoft's plans to "wall off" parts of the memory suggests modifications of the CPU and the memory controller, e.g., by introducing a new capability that is similar, but orthogonal to the well-known "memory ring" concept of the Intel processor architecture. Secured communication between the CPU and the keyboard is likely to require support from a modified chipset.

Intel has declared that LaGrande will be an opt-in technology⁴⁹¹, at least if the new features don't find acceptance in the first place⁴⁹². This has not dispelled concerns about secondary effects such as customer lock-in and loss of privacy, in particular in conjunction with Palladium⁴⁹³. It is relatively safe to assume, though, that LaGrande can be used in conjunction with arbitrary operating systems.

IV.3 Open Source and TCPA

Whether or not TCPA leads to strengthening of customer lock-in to proprietary solutions remains to be seen. If future TCPA based software severely impedes consumers, lack of usability might actually push them to look for alternatives.

IBM as well as HP have shown commitment to both TCPA and Open Source⁴⁹⁴, and we can expect to see TCPA-supporting Linux versions hit the market in the near future.⁴⁹⁵ Both vendors will probably address the enterprise sector first. Other TCPA members declared their support for TCPA-based Linux solutions as well⁴⁹⁶.

There are, nevertheless, compelling questions about the impact of TCPA on Open Source software and its particular development model.

⁴⁹⁰ See: Ortelli (2002).

⁴⁹¹ See: Kanellos (2002).

⁴⁹² See: Bonnert (2002).

⁴⁹³ See: Gaither (2002).

⁴⁹⁴ To recall the core idea of software being "Open Source":

"The source must be available for redistribution without restriction and without charge, and the license must permit the creation of modifications and derivative works, and must allow those derivatives to be re-distributed under the same terms as the original work."

Throughout this article, we use the term Open Source in the generic manner quoted above. See: O'Reilly (1999): 34.

⁴⁹⁵ See, e.g.: Jaeger, Safford, Franke, (2002), discussing the integration of TCPA, Linux, and the Linux Security Modules (LSM).

⁴⁹⁶ See: Krill (2003).

Impact on Free and Open Source Software Developers

Since it seems reasonable to assume that the certification process for TCPA-supporting software will be neither costless, nor without expense of time, three peculiarities of the Open Source community require particular attention:⁴⁹⁷

1. Important parts (approximate 25%) of the developer community do not have significant amounts of money at their disposal. Even small charges of fees for certification may have a de-motivating effect.
2. About two thirds of the community spend between 0 and 10 hours per week developing Free and Open Source software. Every amount of time spent for certification procedures will, presumably, be deducted from the time invested for developing, testing, and debugging code.
3. Many developers are not paid for developing Open Source code. It is hard to imagine those voluntary “hackers”, i.e. sophisticated programmers with strong commitment to pushing information technology to its limits, to invest time and money in order to support business models of industry giants such as IBM and HP.

If a split of the Open Source community is to be avoided, a working model of a TCPA/OS certification process has to be shaped along the sociological structure of the community.

Impact on the GPL

A more puzzling problem is whether Trusted Platform technology will undermine the GPL and other Free Software and Open Source licences,⁴⁹⁸ destroy Free Software, allow the GPL to be “hijacked” for commercial purposes and thereby de-motivate idealistic programmers. The original argument put forward in Anderson⁴⁹⁹ is based on the notion of a “TCPA operating system” and assumptions that full use of TCPA features require proprietary certificates, neither of which is backed up by the specification. On a more general level, however, a valid point has been raised: does the attestation of security properties for Open Source software have implications for its status, flexibility, production process, and distribution?

The attestation of security properties is external to the source code and therefore not subject to the GPL. Attestation can only ever refer to a particular version of the source code: if the code is altered, the attestation of the original code loses its validity.

⁴⁹⁷ We refer to the findings of the “WIDI” study (Robles, Scheider, Tretkowski, Weber 2001) conducted by the Technical University of Berlin, Germany. A follow-up study (Ghosh, Glott, Krieger, Robles 2002) called “FLOSS” and conducted by the International Institute of Infonomics, Maastricht, The Netherlands and Berlecon Research GmbH, Berlin, Germany, showed — with minor differences — similar results.

⁴⁹⁸ See, e.g.: Arbaugh (2002): 78 f.

⁴⁹⁹ See: Anderson (2003).

Evaluators might claim that security validation of Open Source simply adds value to it. However, the validation of this very source code is only possible because it is “there” in the first place and is open to everyone. The source code to be evaluated is “there” by virtue of liberal copyright licenses that allow for a flexible development process, but the assurances that result from evaluations introduce a formerly unknown element of inflexibility. Flexibility as envisaged, e.g., by the GPL seems to be at odds with assurances provided, e.g., by a Common Criteria evaluation.

This presents a serious dilemma, as there could be clear benefits of an Open Source approach to security in general and Trusted Platforms in particular. In order to combine the flexibility of the Open Source development model⁵⁰⁰ with the growing demand⁵⁰¹ for security assurances, new technical and organisational models have to be found.

TCPA, Open Source, and Software Patents

The extent to which TCPA technology and components that can be built on top of it are protected by patents is currently unknown. As far this concerns software patents, it must be emphasised that they have long since been considered incompatible with Free/Open Source software development.⁵⁰² A “source code privilege” as proposed by Lutterbeck, Horns, Gehring⁵⁰³ could prove an essential element for enabling the integration of TCPA and Open Source software.

IV.4 The Trusted Computing Group

The formation of the Trusted Computing Group (TCG) was announced⁵⁰⁴, while we were finishing this text. The TCG has been set up as successor organisation of the Trusted Computing Platform Alliance “*to advance the adoption of open standards for trusted computing technologies*”. AMD, HP, IBM, and Intel are aboard again, as is Microsoft after temporarily having left the TCPA path. In addition, many consumer electronics companies have joined the TCG, e.g., Sony, Philips,⁵⁰⁵ and Nokia.

⁵⁰⁰ For recent advances in the field of “Open Source security” see: Ott (2003a/b); Wright, Cowan, Smalley, Morris, Kroah–Hartman (2002); Pourzandi, Haddad, Levert, Zakrzewski, Dagenais (2002).

⁵⁰¹ E.g.: from July 1st, 2002 on, all U.S. government acquisitions of IT systems processing sensitive data must be evaluated and validated according to the Common Criteria or equivalent. See: <http://www.oracle.com/corporate/press/1623351.html>.

⁵⁰² See, e.g.: Gehring (2003).

⁵⁰³ See: Lutterbeck, Horns, Gehring (2000).

⁵⁰⁴ See: Fisher (2003).

⁵⁰⁵ In fall 2001, Sony Corp. of America, Philips, and Stephens Acquisition LLC jointly bought Intertrust, holder of many trusted systems and DRM technology based patents. In the aftermath, the EU commission investigated potential negative impacts of this new joint venture for the DRM market and concluded “*that the transaction raises no serious competition concerns.*” Cf. Monti (2002): 5.

Jim Ward, chairman of the TCG, describes the aim of this organisation as follows:⁵⁰⁶

“Open standards, widely supported, will accelerate the design, use, management, and adoption of standards-based trusted systems and solutions that are urgently needed to meet the challenges of an increasingly inter-connected world.”

In order to promote this approach, the TCG will continue where TCPA has stopped.⁵⁰⁷ Microsoft is founding member of the TCG, which indicates that its NGSCB plans are compatible with whatever the TCG will pursue.⁵⁰⁸

“TCG has adopted existing trusted computing specifications from the Trusted Computing Platform Alliance (TCPA) and will extend and enhance these specifications.”

TCG and DRM?

While the TCG has dismissed any intention to develop DRM standards,⁵⁰⁹ Bill Gates has made it clear that Microsoft’s future operating systems will support DRM functionality,⁵¹⁰ and Microsoft, who considered the TCPA specification as being not comprehensive enough to support their security architecture not too long ago, has decided become a member of the TCG consortium. Given the TCG’s focus to further develop the TCPA specification, we may assume that DRM based on trusted platform technology à la Microsoft is coming closer. This time, however, it may not merely embrace personal computer systems⁵¹¹, but “multiple platforms, peripherals and devices”⁵¹² as well.

V Summary

Given the complete lack of experience with ubiquitous Trusted Platform technology, difficulties of categorisation and a shortage of independent expertise, many open questions remain. However, it is possible to summarised some preliminary observations.

TCPA and Trusted Platform technology is not identical to DRM technology, although both have a common forerunner in the Trusted Systems concept developed in the 1970s. On the other hand, TCPA offers functionality that can be a used to build DRM systems.

⁵⁰⁶ See press release “TCG announced April 8, 2003”, at:

<http://www.trustedcomputinggroup.org/home>. Last visited: 10 April 2003.

⁵⁰⁷ See TCG FAQ at: <http://www.trustedcomputinggroup.org/about/faq/>. Last visited: 12 April 2003.

⁵⁰⁸ See supra note 507. See also: ComputerWire Staff (2003).

⁵⁰⁹ See supra note 507.

⁵¹⁰ See: Schulzki–Haddouti (2003).

⁵¹¹ See: Merritt (2003).

⁵¹² See press release “TCG announced April 8, 2003”, at:

<http://www.trustedcomputinggroup.org/home>. Last visited: 10 April 2003.

Albeit members of the TCPA consortium, Microsoft and Intel appear to have staged a parallel effort to put the vision of a Next Generation Secure Computing Base into action. It is unclear whether this was a contributing factor to finally declare “[d]eath to the Trusted Computing Platform Alliance”⁵¹³ while simultaneously having the TCG raise from the ashes. Equally unclear are the consequences for a PC market already dominated by Microsoft and Intel. They could be severe, given TCPA’s wide support by the industry. Trusted Platform technology is likely to be deployed on a very wide scale. Large IT users such as big enterprises and the civil service are likely to be the pioneers here.

Microsoft’s announcement to make the source code of its nexus “widely available for review”⁵¹⁴ indicates that a huge problem might be lurking at the core of Trusted Computing: Who guards the guardians? How can one be sure that trusted software components are trustworthy indeed and not Trojan horses undermining the system’s or user’s security instead?

Combining TCPA technology with Open Source software might offer the potential to provide more trustworthiness in electronic transactions. Since the code can be subjected to scrutiny, its potential to foster trust is arguably greater than any combination of TCPA and proprietary, closed source software. The accessibility of the source code as such may not be sufficient to give a convincing answer, but its main virtue “openness” suggests itself as a necessary element to arrive at one.

The proliferation of Trusted Platform technology could change the way information technology is used. If Trusted Platform technology such as TCPA wants to be successful in delivering on its promises of bringing about more security, more privacy, and better customer confidence in electronic transactions, good answers have to be found to well-founded critique. Some of these answers may lie in imparting knowledge about the technology to the users.

In other cases, conceptual, technological or legal changes might be necessary. The Internet revolution has demonstrated that values we take for granted can quickly come under pressure in computer-mediated environments. To sustain constitutional values may well require re-regulation of technology, and it may force us to rethink intellectual property protection.⁵¹⁵

The Need for a Political Debate

Western democracies protect freedom of speech, freedom of information, freedom of trade, and other values we attribute to an open society. Technology that mediates the social discourse influences how we think about these values. Over the last years, politicians all over the world have shown remarkable reluctance

⁵¹³ See: Lemos (2003).

⁵¹⁴ See: Microsoft Corp. (2003).

⁵¹⁵ Most recently, Alan Greenspan (2003) contributed to the debate about how to put intellectual resources to most efficient use. He questioned, whether the existing system of intellectual property protection is “*appropriate [...] for an economy in which value increasingly is embodied in ideas rather than tangible capital.*”

to acknowledge this fact. Laws crafted behind closed doors and enacted to favor particular interest instead of the public one undermine the commitment of the majority of people to the “common good” (John Locke) in the long run. A broad, qualified, political debate⁵¹⁶ about how the information society is shaped by technology like TCPA and Palladium is urgently needed.

About This Document

This text documents an ongoing discussion between the authors. Should inconsistencies occur in the argumentation, they are likely to be an unavoidable result of different points of view. In many cases, we had to confine ourselves to short descriptions of important technological aspects and to forego a plethora of details.

The opinions expressed in this article are those of the authors and do not necessarily represent the positions of their employers.

⁵¹⁶ And here we do not mean a salon debate among professional politicians but rather a social discourse of all stakeholders, including the ‘users’.

A.1 DRM Workshop 2000: Summary

This is a synopsis of the 2000 Workshop on Digital Rights Management (DRM) workshop held on 20th and 21st November in Berlin. The workshop aimed at presenting the topical research, bringing scientists of various disciplines together and drawing the attention to the topic “*Digital Rights Management*”. The conference discussed the technical, political, juridical and economic challenges of DRM and the digitalization of intellectual property (IP). It was the intention to provide a forum for discussion between the relevant parties involved: providers of DRM–technologies, content–providers, service–providers, scientists and representatives of various ministries and lobby groups. Only an interdisciplinary perspective could address the emerging issues adequately.

In the United States the Digital Millennium Copyright Act (DMCA) of 1998 governs the usage of technological protection measures like DRM systems and the copyright in the digital area.²⁰⁸⁷ It is based on two treaties of the World Intellectual Property Organization, the WIPO Copyright Treaty of 20th December 1996 (WCT) and the WIPO Performances and Phonograms Treaty of 20th December 1996 (WPPT). About the time of the conference in Berlin (November 2000) the Commission of the European Union (EU) was designing a directive on Copyright in the Information Society which was later published in May 2001.²⁰⁸⁸ Subsequently the directive ought to be implemented in Germany by adapting the former German Copyright Act until Dezember 2002.²⁰⁸⁹ This directive was to prepare the ratification of the WIPO–treaties mentioned above. When the conference was held the final shape of the EU copyright directive could not be foreseen, the situation was quite open.

This first interdisciplinary conference on DRM and its impact on the digitalization of IP was attended by 150 international participants from the various parties mentioned above. However it was difficult to attract fuller attention of artists and users. The musician Smudo — Michael B. Schmidt from the German music group “*Die Fantastischen Vier*” and the self owned label “*Four Music*” was the only one to speak for the artists. The interests of the users were represented — to some extent — by the German Association for Information Technology (FITUG e.V.) and the Chaos Computer Club.

The conference was opened by the greeting of the Parliamentary State Secretary of the Federal Ministry of Economics and Technology, Siegmur Mosdorf. He pointed out that detailed discussion of the legal regulation of the political and legal challenges in the area of the digital copyright and the application of DRM–systems is urgently needed. This is due to the enormous chances of information and communication technologies (ICT) for the national economy and simultaneously the high risk caused by the new technologies. He clarified that the government is willing to meet the challenges.

²⁰⁸⁷ See: *Lejeune* within this book (page 366); *Simons* within this book (page 383).

²⁰⁸⁸ See: *Reinbothe* within this book on page 405.

²⁰⁸⁹ See: *Dreier*, *Nolte* within this book (page 479); *Goldmann* within this book (page 502); *Ulmer–Eilfort* within this book (page 447).

In his opinion, the “*Cyberspace*” can not be a right-free space. Instead, the legal principle of the offline-world have to apply also in the online-world. Mosdorf opposed isolated national attempts, rather called for global agreements and for a global legal framework. He admitted huge political and legal difficulties to reach these aims, e.g. different philosophies of law, cultural divergences and economic interests of the content or ICT-industries are obvious obstructions.

National political decisionmakers have to balance the vital interests of various parties involved, as Mosdorf stated. E.g. he insisted in further discussing the proposal of levies on ICT and blank media, in particular the application of levies must not hinder the spreading of new technologies.

Mosdorf discussed how to react best on these technological developments. The market has to play the dominant role since it reacts faster and more flexible on the rapidly changing technological reality of ICT. However the resulting legal and political challenges can not be left to the market alone. It is the task of the state to establish the basic conditions and the legal framework which enables the balance of interests mentioned above, e.g. public access to information, an important issue, a government has to take care of.²⁰⁹⁰

In addition, Helmut Mattonet, head of department in the Ministry of Science and Research of North Rhine Westphalia, called attention to the role of science and education in developing new applications for the internet and controlling the legal, political and social risks. In his greeting he invited all professionals to invest new ideas and projects in order to shape the innovation process for the benefit of all.

Jennifer Neumann, representative of the Initi@tiveD21, recalled the governmental obligation. With trailblazing projects it should show the route. Furthermore technical developments have to be promoted. The “Initi@tiveD21”, led by industrial leaders in Germany, aims at facilitating the transition from the industrial to the information age. According to the initiative’s perception, ideas, creativity and knowledge will be important export products in the future Information Society. Thus the protection of IP is very important, an issue technology companies want to address by developing copy protection and DRM systems. Neumann criticized that awareness of the value of IP is missing very often on the side of the users of the Internet. The rights of the authors and other rights holders are not respected. She proposed two strategies to improve this situation: public relations activity and copyright education may help, if not, technologies such as watermarking and DRM could help to maintain the claims of the rights holders. In summary, establishing a legally respectful behavior of a large majority of users should be a realistic target.

Prof. Dr. Andrew M. Odlyzko from the Digital Technology Center of the University of Minnesota (at the time of the conference at the AT&T Labs-Research USA, Head of the Mathematics and Cryptography Department, USA) delivered a keynote on “*Stronger Copyright Protection for Cyberspace: Desirable, Inevitable*

²⁰⁹⁰ See: Article by Böhm (page 520); Dreier, Nolte (page 479); Günnewig (page 528) within this book.

and Irrelevant". He argued that the results of the conflicts between the content providers and the users of digital goods will not play the most important role. Furthermore it is to be expected that on the electronic market place for digital goods the regulations of the copyright law will be of minor importance in future. Rather, technological, economic, sociological and political factors will dominate the way how digital content is sold. Economics and technology will enormously widen and facilitate the access to information in future. In view of the explosion of information governmental laws will turn out to be too inflexible and too slow. He expects content providers to find out that they probably do not need stronger copyright protection. In his opinion, an efficient Electronic Commerce will make customisable contracts much easier to arrange. Competition would also make tight restrictions inadvisable. "*Reduced barriers to entry and reduced costs do bring about a much more competitive market for most information goods*", said Odlyzko. He proposes to put more emphasis on contract law rather than on copyright law. Contract law seems to have the enormous advantage of higher flexibility and to be suitable to settle most legal issues.

In the panel "*Entertainment and Publishing Industry: Requirements, Visions and Plans*" representatives of the content providers were given space to describe their demands on the distribution of digital goods via DRM systems. Markus Böhm, previous Director Sales Europe at Bertelsmann Digital Rights Management Company Digital World Services, Vaughn Halyard, Senior Vice President New Media and eBusiness Strategy, Buena Vista Music Group, The Walt Disney Company, USA and Martin Weinert, Vice President Informationmanagement from Kirch Holding spoke for their companies. They classified DRM systems as an important instrument to secure investments of content providers and to enable new business models for the digital area.²⁰⁹¹

Dr. Leonardo Chiariglione, CSELT, Head of Multimedia Services and Technologies Division, Italy gave a lecture on "*Intellectual Property in the Multimedia Framework*". He provided an technological overview of the work of the Secure Digital Music Initiative (SDMI), and of MP3 and MPEG resp. the audio- and video compression. Chiariglione reported, in particular, on the standardisation of the compression technologies. His comprehensive paper can be downloaded from the conference website <http://www.digital-rights-management.org>.

DRM systems providers presented their approach to tackle the copyright problem on a panel moderated by Prof. Andreas Pfitzmann from the University of Dresden. Dr. Susan Wegner and Hans-Joachim Scheidemann of the T-Nova / Berkom, a subsidiary company of the Deutsche Telekom AG, presented "Music on Demand", a online distribution platform for music. Koos Middeljans reported on the DRM- and content-distribution activities of the Dutch company Philips Digital Networks. Dr. Kevin McCurley (IBM Research, USA) described in his talk three substantial components of a IBM solution for copyright protection where he showed how to adapt "*legal standards to match the reality of the day,*

²⁰⁹¹ See: chapter 3 (economics) and the article by *Gooch* within this book on page 16.

technological innovation to inhibit theft and deliver a satisfying product, and business creativity to grow the business in the face of change". Andrej Budo-Marek from ContentGuard (joint venture of Microsoft and Xerox) presented the implementation of a ContentGuard-DRM-solution. He showed the functionality of the platform "ErWin". This platform secures content of the Volkswagen AG (car industry). Ed Fish from InterTrust Technologies, USA, spoke about the current development of the company's pioneering DRM system.

This Californian DRM-technology-provider also sent Dr. Stuart Haber to give a talk on the conference. Then he was a member of the Research Lab (StarLab) and reported on "*Cryptographic Techniques for Digital Rights Management*".²⁰⁹² In his talk Haber described the DRM-technology of his company as well as DRM-systems in general and outlined the impact on the issue of "fair use". He was opposing the misapprehension that "the end of intellectual property" had come in the Internet Age because of a claimed uncontrollability of IP. Even "the end of fair use" has not yet come, being an issue of controversial debates. "These and similar apocalyptic visions are inspired by an absolutist interpretation of various technologies, whereas in reality the picture is not so simple and clear-cut."

Dr. Fabien Petitcolas from Microsoft Research Great Britain delivered a talk entitled "*Watermarking: why bother?*". He described up-to-date watermarking systems which are designed to help protecting digital goods.²⁰⁹³

Prof. Dr. Karlheinz Brandenburg of the Technical University Ilmenau and Director of Fraunhofer IIS-AEMT (Working Group Electronic Media Technology) gave a lecture on "Technological Aspects of Electronic Media". He is one of the main developer of the audio coding system MP3, most prominent to survey the developments in the compression of audio files and of technologies used for the electronic distribution of intellectual property (IP).

In his talk on "*Pay TV Piracy: Lessons Learned*" Matthew Carter from Cryptography Research Inc., USA concentrated on giving an overview of fundamental methods which he illustrated by several examples. Carter pointed out mistakes which were made during the transition from the analogue to the digital television. Especially the music industries would make similar mistakes right now. The Pay-TV-companies assumed that the so called pirates would not have the set top boxes and therefore could not be in the position to decode the encrypted Pay-TV-Signal. They have thought that the corresponding encryption system would be something like a "global secret" that nobody could solve because of its very good protection. Carter showed these companies to be wrong because hackers figured out the inverse function of the set top boxes. The pirates had built their own set-top-boxes. At this point of time, the industries should have taken a step back and should have re-evaluated their approach, Carter suggested. But they did not as Carter said. Instead they said "I have a great idea: Lets just change the function." But that did not work at all. The Pirates just built different boxes with different functions. This goes on and on and it is a footrace. So

²⁰⁹² See: *Herre* (page 93); *Spenger* (page 62); *Guth* (page 101 and page 150); *Rump* (page 3) within this book.

²⁰⁹³ See his article on page 81 within this book.

far any system has been hacked sooner or later. Tamper resistant devices could reduce the problems of the so called piracy. However in November 2000 no such device exists. Possibly it would never exist, as Carter stated.

New systems for the protection of digital goods would be needed according to Carter. At the time of his lecture, he described the situation as follows: *“There is no system you can point to that says ‘hey, this is what we should do.’ If we could only all build this, the world would be great.”* Various problems hinder the development of such a system, e.g. perfect clones of an authorized decoder will always work. The obvious approach for an attacker, in the area of Pay-TV-Systems, is to try to make a nearly perfect close copy of the decoders. He suggest that it would be good for a protection system to implement revocation of the encryption and decryption keys. It has to be possible to revoke the keys, Carter demanded. Otherwise pirates could use the keys themselves after they are released. In respect to a software based approach of a protection system Carter said: *“If you gonna do this in software, give up, don’t bother. [...] When you are programming on a PC you are programming in a fish tank. Everyone can see what you are doing. You are not able to produce secure software on a PC”*.

As one the mayor problems in the digital content distribution Cater mentioned that most users do not feel a moral dilemma when using illegal software and devices as well as in the application of illegal content. A huge demand for content seems to provoke a huge demand for piracy. The primary motivation for the so called pirates is not to gain money by the illegal content. Instead, they are seeking the intellectual and technological challenges of breaking protection system or delivering illegal content. He arrived at the following conclusion: *“If your goal is to invent an unbreakable system, then indeed the problem is not solvable. If your goal is the minimize loss, then your problem can be solved. This is inherently a business problem. The basic thing here is, if the attackers cost is great than his gain, then your problem is solved.”* According to Carter two approaches exist to render the legal actions more attractive. The first one is to increase the costs for the pirate to break the system. This aims at making repeated attacks very expensive. If the technological protection is broken once, the resulting information gained on the side of the hacker/cracker should be low, so that he could not use this information for a further circumvention of technological measure. A second approach is to decrease the revenues of attacks, e.g. by revocation.

Dr. Barbara Simons, past president of the Association for Computing Machinery USA, delivered a keynote on the effects of copyright acts and the application of technologies on public libraries.²⁰⁹⁴

In the podium discussion *“Legal and Political Processes in Germany and the EU”* the implementation of the EU copyright directive into German copyright law and the digitalisation of IP were in the focus. Martin Cronenberg, Head of department in the Federal Ministry of Economics and Technology, moderated the discussion. On the panel Volker Schöfisch of the Federal Ministry of

²⁰⁹⁴ Her essay within this book on page 383 takes up again the theme of her talk at the conference.

Justice, the legal scientist Prof. Dr. Dietrich Harke of the University of Applied Sciences Darmstadt, Birgit Weise–Montag of the European Commission, Administrator Copyright and Neighbouring Rights and Dr. Kathrin Bremer of BITKOM (Federal Association Information Economy, Telecommunication and New Media) presented their point of views. It was agreed that the national laws of the member states of the European Union have to be adapted, also, that rights holders have to be remunerated appropriately was questioned by none of the participants. However dissens arose as to the question how to allocate the remuneration — by collective and flat–rate remuneration systems, or by an individual remuneration system which depends on DRM technology.²⁰⁹⁵

Andy Müller–Maguhn, representative of the Chaos Computer Clubs²⁰⁹⁶ and ICANN–director, spoke on “*The End of Control of Non–Material Goods in the Internet–Paradigm*”. He started with the statement that the control of non–material goods in the internet could never be complete because protection systems can be broken easily and quickly by intelligent attacks. Therefore any remuneration system should be based on the free flow of information and not on a control sheme. Needed are alternative value chains to be developed by content–providers, scientists and technicians. In this connection he referred to the model Street Performer Model²⁰⁹⁷ by Bruce Schneier.

The final panel “*Digital Rights Management for Music*” on the challenges and the future of the digital distribution of music enabled by DRM–systems brought together Dr. Martin Schaefer, of The German National Group of IFPI e.V., Prof. Dr. Jürgen Plate, Chairman of the German Association for Information Technology (FITUG e.V.), Smudo — Michael Schmidt, Artist & Repertoire FourMusic, artist of the music group “*Die fantastischen Vier*”, Lars Gollnow of Gnutella.de, Georg Oeller of GEMA²⁰⁹⁸ and Christa Haussler, Vice President New Technology von BMG Entertainment. Smudo expressed the need for a strong protection system as well as the help by professionals — like “Artist and Repertoire” (A&R) — enabling the artists to develop their full creativity. Further issues ranged from technical provisions for tracing illegal content (Right Protection System of IFPI) up to unlimited access to information as demanded by Plate and Gollnow. According to Oeller collecting societies as GEMA will still play an important role for remuneration of copyright exemptions in the digital area. Hausler reported on the current situation concerning the “Bertelsmann–Napster–deal”²⁰⁹⁹.

At the end of the first day all attendees enjoyed a wonderful evening in a restaurant in the “Reichstag”, where the German Parliament is located. It helped to establish or deepen business relationships between participants.

²⁰⁹⁵ This aspect is covered in essays *Ulmer–Eilfort* (page 447) and *Günnewig* (page 528) within this book.

²⁰⁹⁶ Association of hackers and media activists.

²⁰⁹⁷ See: Kelsey, Schneier (1998).

²⁰⁹⁸ Collecting Society for Musical Performing Rights and Mechanical Reproduction Rights.

²⁰⁹⁹ Note. Bertelsmann invested into Napster.

The workshop was organized by the sub-projects “*Protection of digital goods — Schutz digitaler Güter*” (located at the Math Department of the University of Dortmund²¹⁰⁰) and “*Coordination and management of the Research Alliance*” (European Institute for IT-Security Bochum²¹⁰¹) of the Research Alliance Data Security North Rhine-Westphalia²¹⁰² in cooperation with the Federal Ministry of Economics and Labour (formerly Federal Ministry of Economics and Technology²¹⁰³). The conference took place in the Federal Ministry in Berlin. The workshop was generously funded by the Ministry for Science and Research of North Rhine Westphalia (formerly Ministry for School, Science and Research²¹⁰⁴).

The program committee consisted of Prof. Dr. Eberhard Becker (Math Department of the University of Dortmund)(programme chair), Dr. Tomas Sander (then at InterTrust), Petra Henseler and Dirk Günnewig (organisational chair) (of the European Institute for IT-Security of the University of Bochum). Marcus Heitmann was part of the organisational team.

Conclusion

The workshop showed, as a first result, that much further research is needed. This is true for all disciplines involved — mathematics, engineering, economics, political science and legal science. Rash and non-balanced political solutions for the complex topics may turn out to be harmful and may lead to disadvantages for the German ICT- or content industry and their competitiveness on the German, European and international markets. Public access to the wealth of information has to be guaranteed. Law or regulations that are socially not understood or accepted will lose their relevance.

²¹⁰⁰ See: <http://www.digital-rights-management.org>;
<http://www.uni-dortmund.de>.

²¹⁰¹ See: <http://www.eurobits.de>.

²¹⁰² See: <http://www.datensicherheit.nrw.de>.

²¹⁰³ See: <http://www.bmwi.de>.

²¹⁰⁴ See: <http://www.bildungsportal.nrw.de>.

A.2 DRM Conference 2002: Summary

I Introduction

Since the first workshop in November 2000 there have been considerable developments in the fields of “*Copyright for Digital Goods*” and “*Digital Rights Management*”. Due to this fact it became necessary to organise another conference conveying the new status. It was held in Berlin in the Haus der Wirtschaft (house of industry). The interdisciplinary and international conference on “*Digital Rights Management– Strategies for Technological, Legal and Political Solutions Regarding Digital Goods– Focussing on the European Copyright Directive*” took place on January 20–21, 2002. As in the case of the previous workshop it was organized by the Research Alliance Data–Security North–Rhine Westphalia within the frameworks of its projects “Schutz digitaler Güter” (Security of Digital Goods) and “Management des Verbundes” (Research Management). This time, we could win the “Deutsche Industrie und Handelskammertag” (the German Chamber of Industry and Trade) as a co–organizer²¹⁰⁵.

The development of the concept was in the hand of Prof. Eberhard Becker (Universität Dortmund), Dr. Stefan Bechtold (Universität Tübingen and Stanford University), Dr. Tomas Sander (InterTrust StarLab then) and Dirk Günnewig who also operated as the organisational chair. The conference as well as the research alliance were supported by the Ministry of Science and Research of North–Rhine Westphalia²¹⁰⁶.

The conference joined politicians with leaders in the economy and researchers. This feature alone “[. . .] *has to be considered as a milestone in the development of digital rights, in the discussion of intellectual property, its protection and usage*” as the State Secretary for Science and Research in North–Rhine Westphalia, Hartmut Krebs, put forward in his welcoming speech.

The conference dealt with the following four topics: the technological, the economical, the legal and the political aspects of digital content and the use of DRM systems. The timing of the event was perfect: the European Copyright Directive was about to be implemented into national law. To be able to discuss details of this transfer the organizers had decided to select the German situation as an example which allows a close analysis of the full spectrum of interests and conflicts resulting from such an implementation. Therefore, various associations, companies and collecting societies were invited to present their points of view and to discuss political and legal problems. It was a major goal of this conference and of this volume, to obtain a most complete picture.

The conference was attended by about 250 participants, 100 more than at the first workshop in 2000. This time the public showed an increased attention to the

²¹⁰⁵ Further corporations with media.nrw and GITS AG (Company for IT–security, Bochum).

²¹⁰⁶ See: <http://www.datensicherheit.nrw.de>; www.bildungsportal.nrw.de

topic and the echo in the media was much more intensive: about 20 journalists were present at the conference and published reports on the meeting.

There are good reasons for this increased interest. First of all, the European Copyright Directive²¹⁰⁷ had been passed after the first conference in 2001. At the time of the meeting in November 2000 the Directive had existed only as a draft. Now the political conflicts between various parties could be dealt with more precisely and directly²¹⁰⁸. Now it was apparent which legal situation one had to face and all players involved had already carried out a detailed analysis of the consequences. Therefore, the second conference was perfectly timed as it took place at a time when the German Government was working at the implementation of the EU–Copyright Directive by amending the German Copyright law. In this period, all parties were actively concerned with lobbying to influence the final wording of the German law.

As previously said, the organizers never had the idea to use the conference as a political manoeuvre. It was rather meant as a forum for the parties involved. The panels dealt with the impact of the anti–circumvention regulation²¹⁰⁹, with the models for “*collective vs. individual remuneration*”²¹¹⁰ and with the role of the collecting societies in the digital area. The question of “fair use” of digital information for the sake of education and research, although of fundamental importance, was not dealt with at the conference. It has to be mentioned however that this issue turned out to be one of the major obstacle in amending the German law²¹¹¹.

After the first conference new developments have taken place from the technical point of view and regarding the legal and political aspects of DRM systems. Providers of DRM systems had been able to present practical systems that could handle the distribution of digital goods as well as the management of the rights of the content owners and producers. These systems had been investigated from an engineering point of view, at least in a preliminary way, and this assessment was to be made public on the conference.

Due to limitation of space and time not all interested persons, groups and associations could be invited. Most of them sent representatives, at least. However, unfortunately two groups were not present at the conference since they lack a well structured organisation: the users (of digital goods) and the artists who are using the Internet as a distribution channel²¹¹². Any further conference should try harder to invite them in a good number to learn more about their points of view.

²¹⁰⁷ Cf. Directive 2001/29/EG of the European Parliament and the Council Mai 22. 2001 for the harmonization of certain aspects of the copyright and the applied protective rights in the information society.

²¹⁰⁸ See: *Günnewig* within this book on page 528.

²¹⁰⁹ See: *Dreier, Nolte* (page 479); *Goldmann* (page 502); *Lejeune* (page 366); *Günnewig* (page 528) within this book.

²¹¹⁰ See: *Ulmer-Eilfort* (page 447); *Günnewig* (page 528) within this book.

²¹¹¹ See: *Böhm* (page 520); *Günnewig* (page 528) within this book.

²¹¹² See: *Günnewig* within this book on page 528.

II Technological Aspects

Content provider tend to offer their legally protected digital goods as premium content. However, since the beginning of the Internet era illegal copies have been available on the web and owners have almost no chance to get their revenues. To remedy this drawback the use of DRM systems has been suggested. They are expected to be capable of efficiently protecting digital goods by stopping illegal use. Moreover, they seem to offer new business models to the content owner by enforcing individual regulations of use on the side of the users²¹¹³.

During the conference, Intel, Digital World Services, IBM, Adobe, Info2clear, InterTrust Technologies and Gemstar eBook demonstrated their DRM systems. The individual presentations of the above competing technology provider showed, nevertheless, that they join in the same idea: DRM systems have to allow access to any content, at any time and at any place. According to the new paradigm a user should be given the option to get access to his preferred content on any device. The access to content should not be any longer restricted to the use of a certain device.

It was pointed out that DRM systems may allow a much wider range of applications than just the distribution of music, videos and text. Examples are intranets in companies or administration where often the problem occurs that access to documents or files has to be limited. DRM systems enable to define the group of authorized persons precisely and automatically. Interesting applications can be expected for example in the communication system between a headquarter and the various branches of a worldwide operating enterprise. Other scenarios are concerned with the use of software in education.

Representatives of technology providers discussed which requirements DRM systems have to meet. Very often political decision makers or other parties involved require particular functions to meet their demands. Or, technology providers are asked to assess the type of rights handled and controlled by their systems. In several lectures the participants emphasized that the technology is neutral as to its final function. But it allows extensive adjustments of applications and business models to specific requirements.

II.1 Security Aspects of DRM Systems

Supported by the DRM technology providers, the industrial association of ICT companies BITKOM does not lessen its political lobbying efforts to ensure that DRM systems are ready for a widespread employment. Critics, most of them from the collecting societies, doubt that. One of their main concerns is that DRM systems do not offer enough security.

Dr. Hannes Federrath from the Department for Computer Science at the Technische Universität Dresden (today: Institute for Computer Science, Freie Uni-

²¹¹³ A description of the component of DRM systems can be found in chapter *Technological Aspects*.

versität Berlin) and some of his colleagues have been working on the security of DRM systems. After the conference he published a security analysis for DRM systems, which he also deals with in his lecture titled “Science Evaluation of DRM Systems”.²¹¹⁴

In his lecture he explained that there actually are no DRM systems, which do not — usually unintentionally — leave a loophole for uninvited guests, such as hackers or just naive users. He illustrated some weak points, which Hauser and Wenz also deal with in their contribution to this volume.²¹¹⁵

Federrath pointed out, that software-based DRM solutions do not offer as high a level of protection as hardware-based solutions. Usually the latter are not used due to cost concerns. In addition, they are not practical for the consumer market, especially when these customers use PCs. Adequate hardware components would have to be installed in the consumer’s PC.

According to Federrath’s analysis, all DRM systems have numerous open flanks, which present no real obstacle for “serious attackers”. His conclusion was that DRM systems offer only limited security and that all systems can be broken.

Some representatives of the DRM technology providers responded to Federrath’s comments, claiming that they were not interested in protection against hackers with criminal intent but against large masses of pirated copies. This piracy can be stopped by the protection mechanisms integrated in the DRM systems.

II.2 Standardization

Considering this vast number of DRM technology providers in the market and the numerous components of which DRM systems are made of, the standardization of DRM systems and its components is of great importance. MP3 and MPEG are good examples for successful standardization.

The standardization is of great importance for the distribution of digital goods in the consumer segment. End devices with limited memory size do not provide enough memory capacity for the software of numerous different DRM systems. Different content providers are able to use different DRM systems. A consequence could be that a compilation with 30 songs from the charts with 30 different people holding the rights would require 10 different DRM systems. In this case ten different DRM systems would have to be installed on the end device to enable the consumer to use the entire content. Standardization allows different formats of content to be used on one end device.

In his lecture on the subject “DRM Standards” Niels Rump, Senior Consultant at Rightscom Ltd., a London consulting firm, recommended that in the architecture of DRM systems two elements should be taken into account. First of all, the identification of digital goods is subject to a homogeneous scheme. These digital goods contain the legal utilization regulations in the form of metadata. In the second place, attention has to be paid to the corresponding description

²¹¹⁴ See: Pfitzmann, Federrath, Kuhn (2003)

²¹¹⁵ See: *Hauser, Wenz* within this book on page 206.

of the content itself. If these design requirements were ignored, not readable Metadata, not integrated components of DRM systems or a different description language²¹¹⁶ would reduce the readability of the content. It would not be possible to use the same content on different DRM systems.

Rump refers to the Rights Expression Languages (REL). Here the rights of right owners and/or content providers are laid down in a machine-readable way. These rights are realized by the DRM system. A standardization in this field would have positive effects on the standardization of DRM systems. These homogeneously defined rights could be used as a basis for the different DRM systems to display their specific effects. Corresponding standardization efforts can be seen. In this context programmers ask for common (rights) data dictionaries.

Up to now the rights — especially on an international level — have been expressed differently, causing problems with regard to the interpretation. To resolve these (international) differences a central compilation of possible expressions is favoured world-wide. This compilation guarantees interoperability with regard to the legal nuances of potential utilization rights and thus to the accessibility of the digital product. Furthermore, the REL contains translating mechanisms which play an important role in the distribution of digital products within different DRM systems.

III Economic Aspects²¹¹⁷

The digital distribution changes the companies' value chain and allows new utilization possibilities. Despite numerous unanswered questions the media industry has to face when using DRM systems, the conference showed the enormous economic interests in the business sector, to spread contents over the net and earn money with it. The representatives of the media industry agreed that the digital distribution promises a market worth thousands of millions for music labels, film producers, publishers, artists and authors.

According to the representatives of the media industry this market can hardly be developed without an effective copy protection and DRM systems. *“But the moaning of the phono industry does not mean that they just pretend to be suffering”*, Peter Zombik, the Managing Director of the IFPI and the Federal Association of the Phonographic Industry, was quoted as saying. The illegal copies cause significant drops in sales and prevent new business models and new distribution platforms. *“Increasing the solvency by supporting the user acceptance is the right way. But when you try to establish a petrol station in a desert where there are oil wells bubbling on both sides of the way, it seems that part of the development has been missed”*, Zombik explained.

²¹¹⁶ An example for such a language is DIDL (Digital Item Description Language) or the language XRML©.

²¹¹⁷ See chap. 3: *Economic Aspects* and its subsections of this book.

But he also was confident that a change for the better is in sight: “*We are not at the end but at the beginning of a development which enables us to merchandise digital goods with a copyright on the free market!*”

At the Berlin conference DRM and copy protection systems were regarded as the saviours in the battle against illegal offers. How extensive and profitable the new digital market can be developed with the help of DRM systems, was stated by Thomas Kleesch from IBM: “*We want to enable the companies to bring digital contents via every media to everybody everywhere and to measure and control the results*”.

Willms Buhse from Digital World Services, a DRM company, and post-graduate student at the Department of General and Industrial Management at the University of Munich, presented possible business models for the distribution of digital goods quoting the music industry as an example²¹¹⁸. He sees clear signs for DRM systems finding their way into business models.

Buhse broke down the costs for digital goods into “first copy costs” and variable costs. “First copy costs” are costs accruing in connection with the production of the first copy of the master tape. In contrast to the physical distribution of music (Audio-CDs, LPs, etc.) the digital distribution would reduce the costs to about 21 %. According to Buhse, the marginal costs and the expenditures of the labels represent about 20 % of the costs for the digital distribution. However, in the field of digital music the production costs are negligible. The main costs are marketing and sales costs.

Thanks to DRM the digital-based media sector will develop a broader range of products or a bigger service package. These additional products could for example be preprint versions of a book or the download of single pieces of music prior to the publication of the album. Buhse predicted that it will soon be possible to download an unknown piece of music directly with the combination of mobile communication provider, right owner, pay system and a content server respectively provider via a mobile phone. With technically standardized formats it should be possible to transfer this piece of music to every end device.

As an example for possible extensions of the service package, he quoted the idea of an eBook that could present the user with, for example, historical backgrounds as animated video sequences.

The visions the representatives of the DRM Technology Providers InterTrust had, still seemed to be very futuristic. Due to DRM systems travellers will be able to take their private living rooms, or rather the media content like books, CDs or movies everywhere with them, without ever physically having to move them.

During the final discussion on the topic “The Future of Digital Content” Markus Schmidt, Chairman of Interactive Media CCSP AG (Springer), explained that the future of the digital content is based on four sectors: digital distribution, digital aggregation, product improvement and business models. The supplier

²¹¹⁸ See chap. 3: *Economic Aspects* and its subsections of this book.

can secure this future with “value content”. For these contents a legal framework has to be built, importance has to be attached to the usability aspects of the technical security systems and the value chain of the media industry has to be optimised. Both accounting information and licence changes must be run through the DRM systems. Due to the different kinds and formats of licences the integration into a rights management system is necessary. Schmidt explained that the future of publishing houses is based on restructuring. The potential of brands in the daily press and in monthly journals has to be utilized for the Internet on a strategic marketing level. For book publishers, whose business he called lousy, stock production (high fixed costs, conversion of potential liquidity into stock keeping) is a problem. Here a streamline principle, a kind of just-in-time-concept should be established.

Dr. Christian Dressel, Head of the E-Security Department at Kirch Holding, emphasized the importance of cooperation models with equipment producers and of a reliable legal framework to enable a safe distribution of digital content. With subscriber systems, for example, one would have the opportunity to get directly into contact with the customer at any point of the rights management or within the value chain. The interplay of conditional access systems and subscriber systems enables an exact addressing of users and consumers. The access for the consumer to the contents could be established everywhere along the value chain. To quote: “*the technical opportunities for individual addressing enables the value chain to be atomised. And this can only be in the interest of all content suppliers.*”

Tomas Sander, at that time member of the research laboratory StarLab of the Californian DRM technology provider InterTrust, explained that DRM systems could be utilized to make the user see the importance of the copyright. This has been lost, now that illegal and free ways of downloading are possible. Apart from that the employment of DRM systems in connection with good business models could stop the user from choosing the free alternative of P2P-networks and make him use the legal offer. According to Sander the fact that it is easier for the user to search for contents, is one of the advantages of the legal offers realized by the DRM systems. In contrast to that, the P2P-networks in which contents with a copyright are illegally exchanged, the user has to deal with different media formats requiring additional software. Apart from that the user often downloads faulty media files. Therefore it is much harder for the user to get the contents he was looking for. DRM helps to reduce these conversion charges to the benefit of the consumer. As Sander sees it, the copyright guarantees the wide spectrum of and the access to the digital content adequately controlled by DRM.

Buhse and Schmidt see the user experience as the most important aspect. Therefore future DRM systems have to be equipped with additional functions to combine the offered contents with a positive user experience (with different implementations). User experience and the readiness to offer such systems would increase the consumer’s acceptance. Up to now acceptance and willingness to pay have been missing. This can be reduced to the degree of the user’s contentment

with the offered offline and even the illegal applications. Value-added contents would be incentive.

Buhse described the fact that the technical systems provide the right owner with an instrument of control for procedures like the issuance of the right of use, enabling him to control the access and the application independently, as an innovation of digital distribution. As far as that goes the author does not need middlemen in the digital distribution to get into contact with the consumer and to sell his work.

Independent artists are also in the position to choose their source of income and to control the payments. According to Buhse DRM systems could enable them to establish their individualized market place in the Internet. Therefore the establishment of international cooperations, contacts and relations would be easier than it has been via the traditional distribution routes.

That part of Buhse's lecture was not accepted without contradiction. Dr. Peter Hanser–Strecker, President of the Schott Musik Verlag (music publisher) saw the present practice from a different angle. He rather saw the author standing alone. Technicians, lawyers and consumer are relying on the DRM security mechanisms and their effectiveness. Up to now these efforts have not been successful. According to Hanser–Strecker they can all be cracked. He pointed out that parts of the publishing industry are complaining about a 100 % slump. As long as the authors are not protected effectively in the digital net, no money can be made in the Internet.

Hanser–Strecker identified the speed with which the (trading) conditions are changing as the actual problem. The dynamics on the Internet are three times as fast as those of legislation. The author is in a very difficult position: “*Unfortunately the release of the publication in most cases is the last income possibility*”. Buhse's contribution (together with Amelié Wetzel) to this volume²¹¹⁹ is based on his lecture at the Berlin DRM conference.

IV Legal Aspects²¹²⁰

What is carelessly called the digital content is nothing else but the life blood of the Internet, namely the content with a copyright, Dr. Jörg Reinbothe, European Commission, DG Internal Market / Head of Unit Copyright and Neighbouring Rights, explained in his lecture. In this sense the digital content is a cultural asset to be protected. It's security in the digital net is important to maintain quality and to guarantee safe access. According to Reinbothe, the copyright thus ensures a wide spectrum and the access to the digital content, appropriately controlled for all parties by DRM.

In 1996 the World Intellectual Property Organization (WIPO) enacted two international treaties WIPO Copyright Treaty and WIPO Performance and Phonograms Treaty at the diplomatic conference on certain copyright and neighbouring

²¹¹⁹ See: *Buhse, Wetzel* within this book on page 271.

²¹²⁰ See chap. 4: *Legal and Political Aspects* and its subsections of this book.

rights questions. These treaties were meant to establish a directive for the endorsed countries to adapt national copyright laws to the challenges of the digital technologies. The main issue is the enactment of an anti-circumvention regulation of technical measures, to protect works with a copyright.

The anti-circumvention regulation is important to secure the employment of copy-protection mechanisms and DRM systems which guarantee the security of the copyrights and enable new business models. The USA enacted the DMCA in 1998 and the European Union followed with the EU Copyright Directive in May 2001. This directive was to be implemented into EU law until the end of December 2002. Both, DMCA and EU Copyright Directive include anti-circumvention of technical measures.

At the conference it became more than clear that there are considerable legal and political conflicts involved in the process of implementing the EU information directives. These conflicts became obvious in the introductory jurisprudential lectures as well as in the political discussions. Prior to dealing with the conflicts of interests of representatives of important affected groups on the second day, the first day had been filled with judicial lectures building the legal foundations. The copyright in the USA²¹²¹, in the EU²¹²² and in Germany²¹²³ were described and compared.

IV.1 DRM and US Copyright

The purpose of the lecture of Prof. Julie E. Cohen from the Law Centre at the Georgetown University Washington was to report on the experiences made in the USA with DMCA since 1998 and to outline the law.²¹²⁴ The DMCA contains regulations similar to the EU Copyright Directive for the anti-circumvention of technical measures. Therefore experiences made in the USA are of interest for the national implementation within the EU.

The law was also subject of various panels. Critics used it as an opportunity to point out the mistakes made in the development of the copyright in the digital field.

Cohen talked about the negative aspects of the DMCA. According to her the DMCA restricts the rights of the user. She criticized the problems caused by the injustice of the DMCA as well as the ones caused by the employment of DRM systems. The aim of DRM systems is to restrict freedom. Although it would technically be quite possible to design DRM systems in a way “*that protect models away from making money and to preserve some user freedoms and innovator freedoms which are attacked by legal systems*”.

²¹²¹ See: *Lejeune* (page 366); *Simons* (page 383) within this book.

²¹²² See articles in chap. 4.2 of this book: *Protection of Digital Content and DRM Technologies in the European Union*.

²¹²³ See articles in chap. 4.3 of this book: *Protection of Digital Content and DRM Technologies in German Copyright*.

²¹²⁴ See chap. 4.1: *Protection of Digital Content and DRM Technologies in the USA* and its subsections of this book.

Cohen pointed out that the DMCA leaves room for interpretations. Here she referred to the imprecise or rather unclear wording of the DMCA “*substantial non infringing use and limited commercial purpose or use*”. As well-meaning as the phrasing “*limited commercial purpose or use*” might be with regard to the private copy as fair use, it could also be interpreted to legitimise the prohibition of certain technologies in the USA.

Cohen claims that despite the anti-circumvention of technical measures the user should maintain the right to act independently where the economic implications are minimal. Both, the US copyright law DMCA as well as the EU Copyright Directive include such regulations. In certain cases the anti-circumvention regulations can be ignored according to the exemption of the copyrights. Cohen listed several examples for such exceptions: public libraries and educational institutions, disabled persons, scientists and consumers (private copy). But the respective regulations in the DMCA do, however, show some discrepancies.

In this respect the DMCA can not serve as a model. The jurist sees an inconsistency in the ban of the circumvention of access controls or rather in the ban of “*trafficking devices for circumvention*”. According to DMCA the implementation of effective protection measures in this case requires the use of DRM systems or other technical measures. When systems do not meet the requirements and can therefore be bypassed they do not reach the level of effectiveness required by the law. The ban of the circumvention of this measure does not take effect here and the hacking of such systems for security reasons would be allowed. The American law attaches the definition of an “effective system” to the necessity to use passwords, keys and/or algorithms when accessing contents via the technology. The same can be applied to the availability of data and profiles. Personal data are subject to the individual decision of the person concerned. Therefore exceptions which allow anonymous surfing in the Internet should be included in the DRM systems.

One of the legal fallacies in the decisions of the American law courts concerning DMCA is contained in the anti-circumvention of technical measures. According to the regulations technical measures can be employed by the right owner as a means of control. Therefore the access to contents protected in such a way can be individually controlled. Cohen warned that these technologies are not to implement exclusive rights which would allow to rule out for example the right of reproduction for private use. Allowances for exceptions to this exclusive right should be allowed for in the DRM systems. With the anti-circumvention of technical measures American courts considered this safe and controlled access to contents to be a fact. But Cohen considered this solution embodied in the DMCA as critical. It can not be that DRM systems prevent the user — regardless whether it is a private or an industrial user — from getting access to contents or restrict their private reproduction.

IV.2 DRM and Copyright in the EU

The lectures about the EU Copyright Directive have been of great interest during the conference. The guideline has to be implemented into the national copyright acts of the EU member states.

At the conference Dr. Reinbothe was named the intellectual father of the EU Copyright Directive. As Head of the Unit Copyright and Neighbouring Rights of the EU Commission, DG Internal Market he had an important part in the development of the directive. He reported on the development of the directive and its legislative predecessors, with which the EU tried to harmonize the European domestic market. Following Reinbothe, Prof. P. Bernt Hugenholtz, Institute for Information Law of the University of Amsterdam and the lawyer Marc C. Hansen from the law office Wilmer, Cutler & Pickering, London/Brussels discussed the directive.

“To be called the intellectual father of the copyright directives does not necessarily feel good due to the theoretically existing critics. However, as the saying goes, politics are known to be the art of feasibility. The copyright directives naturally reflect a compromise, too. As far as I am concerned the only possible one between fifteen member states with in parts totally different legal systems especially in the field of copyright which is determined by and aimed at culture anyway”. That is what Reinbothe said after he had been announced as the “intellectual father” of the directive. Reinbothe’s article in this book is based on his lecture at the conference.²¹²⁵ Therefore his lecture is not to be presented here again.

Prof. P. Bernt Hugenholtz from the Institute for Information Law at the University Amsterdam started the criticism of the DRM systems and of the European directive. Related to the article 6 (obligations as to technological measures), paragraph 1 of the EU Copyright Directive he explained: “[...] *this is the longest provision ever seen and very complicated and Reinbothe is not to blame for it. It must be ranked as the worst piece of legislation in European history.*”

Hugenholtz described the danger that the right owner and not the legislator employs the DRM system to determine the range of protection of digital goods. In his lecture Bechtold also mentioned the danger of privatisation of the legal protection, Hugenholtz refers to in this context.

According to Hugenholtz it could happen that digital contents without a copyright are protected by DRM systems. The EU Copyright Directive does not only protect old copyrights but creates a new property right without exceptions and restrictions. Bechtold, too, deals with the fact that use and occupation contracts could break copyright exemptions. In this respect the copyright might have to protect the user and not the right owner against misuse in the future.

Article 6 (obligations as to technological measures) includes the theoretical approach towards a brand new property right (privatisation of the property right). “*La pièce de Résistance*” of the directive is included in this article — the starting

²¹²⁵ See: Reinbothe on page 405 within this book.

point for resistance.²¹²⁶ Thus he predicts the consumer's resistance against the ban of private copies by means of technical measures and the author resistance fighting for a fair compensation.

Following his colleague Dr. Bechtold and his legal thesis, Hugenholtz quoted the metaphor "copyright cast in silicon"²¹²⁷ The technical possibilities of DRM systems enable the content provider to prescribe the conditions under which the contents can be used and to push them through effectively.

In this context Hugenholtz urged to take the rights of the user more into consideration. Due to the abandonment of the "*right to hack*" these rights are in danger when these exemptions work effectively. From the subparagraph 4 of the directive Hugenholtz concluded the clear demand for the governments to make a decision.

The lawyer Mark C. Hansen from the law office Wilmer, Cutler & Pickering regarded the directive as absolutely acceptable. For the areas in which DRM systems allow copies he demanded the collective compensation systems to be abolished. Hansen described the subparagraph 4 of the article 6 (obligations as to technological measures) of the EU Copyright Directive as a tightrope walk between private copy and DRM systems as technological protection measures.

Hansen explained that the exact definition of utilization regulations and standards would result in a tangible solution. It is necessary when operational and above all existing DRM systems are to ring in the slow but certain retreat of flat rate expenditures and compensation systems.

According to Hansen flat rate remuneration models for private copies and other special regulations are to be abolished in the same extend as effective DRM systems are available.

IV.3 DRM and German Copyright

"I am faced with a small problem, for I have nothing new to talk about". — With these words Prof. Dr. Hoeren, Law School of the University of Münster, opened his lecture on the topic "*DRM and German Copyright Law*". But this introduction proved to be an understatement. Hoeren explained his introductory words with the fact that the BMJ had not presented a draft for the realization of the EU Copyright Directive at the time of the conference. He would have loved to present and discuss this draft.

In his following lecture he came up with some news concerning the protection of DRM systems against circumvention and above all the "*protection against DRM systems*". Hoeren mainly criticised that the second aspect had been neglected in

²¹²⁶ His metaphor reminds one of the inexhaustible resistance of the French people during the World War II in whose capital the occupying German regime was brought down.

²¹²⁷ Note: The metaphor is used in the doctoral thesis of Bechtold. See: Bechtold (2002): 277, 279, 370

the political discussion up to now. He outlined the German legal situation and thought about the implementation of the directive into German law.²¹²⁸

He criticised some aspects of the directive and of the possibilities of implementing it into national copyright. At first he pointed out that the right owner can bypass exemption regulations by contract in most cases. DRM systems guarantee the effective enforcement of adequate utilization regulations by the right owner.

In his lecture he criticised that there is not enough time for the implementation of the directive into the laws of the member states. The directive had passed the EU committees in May 2001 and should have been integrated into national copyright acts by the end of December 2002. Considering the pressure put on the copyright amendment he especially regretted that the consumer interests have been neglected. In contrast to the equipment producers or the media industry, the end users have been lacking a powerful lobby up to now. Their voice has yet not been heard by the political decision-makers.

Due to the lack of consideration of all groups Hoeren demanded a wide-ranging “*moratorium*” for the conversion of the directive as well as an “*open discussion*” before “*the job is done*”. Therefore there should be enough room for discussions between the groups involved without being subjected to the imminent implementation deadline. Hoeren required the user rights to be considered more strongly.

According to him it should not be accepted that the users and their interests are not protected as well as those of the right owners. The copyright laws and regulations should protect the user against too restrictive use and occupation contracts and the corresponding DRM systems.

In his lecture he went as far as to demand the restructuring of the copyright without taboos. This restructuring should be based on the principle of freedom of opinion equally embodied in the article 5 as the freedom of speech and freedom of the press. Thus the “*exclusive right to information*” repeatedly demanded by the copyright industry and the content providers needs to be justified instead of the exceptions.

In his lecture Hoeren makes clear that the rights specified as copyright exemptions in the German Copyright Act as well as in the EU Copyright Directive are constitutionally protected. Behind the right of private copy vested in the exemption regulations stands the user’s right of access to the available knowledge.

Later, in a comment during an open discussion, Dr. Elmar Hucko, Departmental Manager in the Federal Ministry of Justice, pointed out that with this directive the Federal Government had to cope with a difficult problem. The directive standardizes indisputable facts but leaves disputable points, like for example the admissibility of electronic press mirror or the private copy for the national legislation to deal with. Above that he criticised that the time period granted to implement the EU Copyright Directive is the shortest ever.

²¹²⁸ See chap. 4.3: *Protection of Digital Content and DRM Technologies in German Copyright* and its subsections of this book. See particular: *Dreier, Nolte* (page 479); *Ulmer-Eilfort* (page 447); *Hoeren* (page 574) within this book.

Besides the lecture of Hoeren legal aspects concerning the German legal situation were consolidated at various panels on the second day of the conference. These aspects are dealt with in a special chapter concerning political areas of conflict.

IV.4 Other Legal Aspects

In his lecture entitled “*DRM Standardization and DRM Regulation*” Dr. Stefan Bechtold spoke against the expositions of Professor Dr. Thomas Hoeren who had previously called the copyright a “*vermiform appendix of the information right*”. Besides the Tübing lawyer Bechtold there were other scientists who did not forecast the death of the copyright. According to Bechtold, when DRM systems come into use, a substantial shift in the meaning of copyrights in the digital field is to be seen. Therefore the copyright does not give as much priority to the copyright as it did before but provides a better protection for the user.

Not referring solely to the German copyright, Bechtold worked out several protection mechanisms which complement each other within DRM systems and which are characteristic for these systems. These are the protection by means of technical measures, the anti-circumvention of technical measures as well as the legal protection by means of use and occupation contracts and technology licences. If we go one step further, patents and industrial secrets will be added.

In this connection he referred to the strained relationship between DRM systems and the customary copyright. According to Bechtold DRM systems can replace the copyright up to a certain degree. But this could cause the copyright protection to be privatised.

Bechtold described an increasing privatisation of the copyright protection caused by the different protection mechanisms being amended. In most cases conditions for the use of the digital contents can be enforced by the content providers. As a result the providers can get rid of copyright exemptions by means of contractual regulations. Competition and innovation capability could be impeded. One of his main statements was that due to privatised legal protection by means of legal technical configurations within DRM systems, users should be provided with the right to protect themselves.

V Political Aspects: Conflicts Concerning Digital Goods and the Employment of DRM Systems²¹²⁹

During the conference several political conflicts were the subject of discussions. Among them were the consequences of the employment of DRM systems for the privacy of the consumer, the consequences of anti-circumvention regulations for the cryptographic research and the question of a future remuneration system in the digital area (flat rate and collective or individual). Furthermore the role of collecting societies in the digital field was discussed.

²¹²⁹ See chap. 4: *Digital Rights Management: Legal and Political Aspects* and its subsections of this book.

V.1 Privacy

Dr. Alexander Dix, Commissioner for Data Protection and Access to Information, Brandenburg, pointed out that DRM systems will endanger the privacy, if all data is collected. His main demand — derived from his description of the scenario of possible risks for the privacy due to DRM systems — was that anonymous and pseudonymous applications are provided for in DRM systems.

V.2 Cryptographic Research

At the time of the conference the consequences of DMCA for the cryptographic research were discussed in the USA. Some controversial law suits were based on the DMCA with the intent of preventing scientists from publishing their research results. The DMCA includes legal regulations which prohibit the production and the distribution of tools for the circumvention of technical (protection) measures as well as the corresponding instructions. Although an copyright exemption for scientific research on technical measures has been provided for in the DMCA, law suits were based on it due to its inaccuracy.

For cryptographic research the security analysis of technical protection systems is of great importance to enable scientific progress. Through analysing the weak points, better protection measures can be designed. Science lives on the exchange of research results. Therefore, sharing information is essential, according to the supporters of cryptographic research on technical protection measures. Opponents see this research as a door for the invasion of the so-called “pirates”, for crackers could use the information to supply illegal P2P-networks with stolen contents.

The EU Copyright Directive also contains adequate regulations for the anti-circumvention of technical measures. The regulations as well as the DMCA go back to the respective directives of the WIPO contracts from 1996.

At the time of the conference, in January 2002, it was feared that similar law suits with the same negative effects would be possible in Europe or rather Germany, when comparable regulations are enacted for the EU member states. At that time as well as in the following political discussions of the implementation of the EU Copyright Directive this aspect was not fully considered.²¹³⁰ Apart from a few scientists no parties involved maintained an acceptable point of view.

In this context the conceivable problematic consequences for the cryptographic research were taken up at the Berlin DRM conference. The two cryptography researchers Dr. Drew Dean, computer scientist at the computer science laboratory, SRI International, and Niels T. Ferguson, MacFergus bc., independent cryptography consultant, illustrated the consequences of DMCA in this field with their progress reports. Cohen reported on the corresponding regulations of the DMCA in the USA and Hugenholtz talked about the probability that similar consequences of the anti-circumvention regulation in the EU Copyright Directive are to be expected for the cryptographic research in Europe.

²¹³⁰ See: *Günnewig* within this book on page 528.

Fergusson and Dean warned the EU member states not to make the same mistakes as the USA. They reported on their experiences with the DMCA. They stated that the threat of punishment keeps them from publishing their research results. In this context the two researchers advised against laws impeding their work in a way that would jeopardize their livelihood.

Besides, these regulations would have negative consequences for the IT-security when impeding the research in this field. No research on technical protection measures would mean that the security of systems can not be tested in a reliable way and that no loophole found by hackers can be determined and eliminated by legal means.

The Dutch cryptography expert Niels Fergusson claims to have hacked the HDCP copy protection²¹³¹. However, he has not published his research results yet, because he fears being charged in the USA due to the anti-circumvention regulations of the DMCA.

Fergusson pointed out that he will be faced with a prison sentence and a substantial fine in the USA after publishing his results. He has the choice of sacrificing his freedom of opinion or his freedom to travel. So far Fergusson has chosen to sacrifice his freedom of opinion as he often has to travel to the USA. As to his hack he only said as much as that it took him less than two weeks to read-out the master-key for the HDCP with little effort after downloading the specifications. Despite the fact that the system, which should protect the transfer of video signals between a PC and a LCD-display has thus been compromised numerous content providers still rely on it. There can be no reliable security analysis without the publication of his research results. Intel simply rejected his report as being unfounded. Fergusson is not allowed to disprove this judgement.

Drew Dean has also encountered negative experiences with the regulations of the DMCA for the anti-circumvention of technical measures. As a cryptographic expert at the research laboratory Xerox Parc he and Ed Felten took part in the hacker competition of the Secure Digital Music Initiative (SDMI) in the autumn 2000. Due to the regulations of the DMCA his research did have consequences. It cost him over \$ 17.000 of legal expenses. In addition he had to relinquish his job at Xerox Parc. At the time of the conference he already worked in the laboratory SRI International. However, cryptography is not longer the focus of his research.

Cohen acknowledged the statements of the two technicians. In her short lecture about the lessons to be drawn from DMCA Cohen referred to the fact that DMCA endangers the freedom of cryptography researchers. The corresponding exception from the fundamental prohibition of circumvention of technical measures is too vague.

But Bernt Hugenholtz, Professor at the Amsterdam Institute for Information Law, gave the all clear in Berlin. "*The reason for the circumvention is decisive*". The cryptographic research could not be the reason for filing a suit based on the EU Copyright Directive.

²¹³¹ High-bandwidth definition content protection.

V.3 Individual in Contrast to Collective Remuneration Systems and the Future of Collecting Societies

In Germany the main topic in the political discussion on copyrights is the remuneration system for use according to the exemption regulations of the copyright.²¹³² Each party involved hoped that with the implementation of the EU Copyright Directive into the German copyright the conflict would be settled according to their specific expectations. The amendment was meant to put an end to conflicts being settled in court.

DRM systems are one of the main arguments the collective remuneration system uses for the employment of adequate copyright exemptions. They are meant to help to replace the collective and flat rate remuneration system with an individual remuneration system. At least that is what the ICT industries²¹³³ hope for. With the help of DRM systems the user should be charged individually for each use of content.

At the DRM conference this conflict was discussed. The different positions were represented at a panel. It dealt with the question if due to the new possibility of individual contractual use regulations offered by DRM systems, the collective remuneration model can be abolished. Participants of the panel were Hans-Joachim Otto (member of the German Parliament, moderator), Prof. Dr. Ferdinand Melichar (General Manager of the collective society Wort), Dr. Martin Schaefer (Bertelsmann Music Group, Vice President Legal Counsel of BMG Europe), Nic Garnett (InterTrust Technologies, policy advisor), Dr. Kathrin Bremer (BITKOM, Legal Advisor), Karola Bode (Compaq Computer GmbH, Director Consumer Products) and Hans-Jochen Lückefett (Hewlett-Packard Germany, Managing Director). The future of collecting societies was discussed at a second panel. Dr. Jörg Karenfort, (LL.M., lawyer at Wilmer, Cutler & Pickering, moderator), Prof. Dr. Jürgen Becker (GEMA — Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrecht (German collecting society), Member of the Board), Dr. Tilo Gerlach (Gesellschaft zur Verwertung von Leitungsrechten mgH (German collecting society), Managing Director), Dr. Nils Bortloff (Universal Music, Universal Holding GmbH, Director Business and Legal Affairs), Fritz Teufel (IBM Deutschland, Manager of Intellectual Property Department) and Grietje Bettin (Member of the German Parliament) took part. Due to the similar aspects these two panels are presented in the same chapter.

Karola Bode, Director Consumer Products at Compaq GmbH, states that in case of a flat rate levy for hardware and blank media the computer industry might go abroad. She as well as Dr. Kathrin Bremer from the industrial association of ICT companies (BITKOM) demands the collective remuneration systems to be replaced with an individual systems which are to be enabled by DRM systems.

²¹³² Concerning the legal aspects of the exemption regulations of the German copyright see: *Ulmer-Eilfort* (page 447); *Dreier, Nolte* (page 479) within this book.

Concerning the political conflicts see: *Günnewig* within this book on page 528.

²¹³³ See: *Günnewig* within this book on page 528.

In the ongoing dispute over the payment of copyright levies for PCs and other electronic devices like CD-writers the computer industry sees no way to relent anymore. According to her the German computer producers can not be competitive on the international market any longer. After all the whole sector is under enormous cost pressure and a levy would cause additional costs in the amount of three or four percent. In the year 2001 Compaq sold 800.000 computers in Germany, so that the levies would add up to 46 million marks. The Compaq manager declared that if the producers actually have to pay this sum retroactively as demanded by the authors and right holder, “it would kill us”. According to Bode, working for the German branch of the American Compaq group, German companies are discriminated.

Bode explained that with the ICT companies threatening to go abroad, “*dramatic topics*” like the loss of jobs and tax deficits are involved. Similar arguments were brought forward by Hans-Jochen Lückefett, Managing Director of Hewlett Packard Germany. The introduction of a new levy for IT devices would be “obstructive”. He complained: “*It can not be, that above all the IT industry has to serve as a cash cow*”.

Bode described the two alternatives the hardware producers have, to deal with this levy. The first would be to form liability reserves. But this would cause problems for companies with parent corporations in the USA. According to Bode the structure of the American accounting system alone would prevent this from being realized. The second alternative would be that the companies face the cost pressure and try to survive on the German market.

The ICT companies preferred an individual remuneration system to a flat rate levy. An essential argument of the equipment industry was that according to the copyright the flat rate levy is only to be regarded as the second-best solution, when an individual remuneration is not possible. That had been the reason for the decision in favour of a levy on devices like for example tape recorders. In contrast to the collecting societies the representatives of the hardware industry explained that due to operational DRM systems, this levy is not advisable anymore. An individual remuneration system would be the only appropriate one to guarantee the interests of authors and right owners. Lückefett as well as Bremer and Garnett from the DRM technology provider InterTrust think that adequate systems are ready for the widespread usage.

Prof. Dr. Ferdinand Melichar, General Manager of the collecting society Wort, spoke against these arguments. He pointed out that the collecting societies had already been waiving remunerations for PC for five years. The ICT industry did have enough time to adapt its business models. The flat rate levy is no discontinued line. Even if the individual accounting methods for contents with a copyright is to amend the present regulations the only thing to discuss will be the levy itself. This levy is too low anyway.

According to the GEMA (German collecting society) representative, Prof. Dr. Jürgen Becker (member of the board) the technology providers “are fighting a rose war” with the collecting societies. The whole business of the collecting societies can not be transferred to DRM systems. There still has to be a central

coordinating body managing the world repertoire for content providers and securing access for users. With the words “Not versus but and” he described the necessary coexistence of the two systems. This depends upon effective and secure DRM systems. But this requirement has still to be met.

A representative of the collecting societies stated that the digital distribution of contents with a copyright require flat rate models. In this connection Dr. Nils Bortloff, Director Business and Legal Affairs at the Universal Holding GmbH of Universal Music stated the following: For the market value of digital goods depends on the expected sales which on the other hand depend on the licensing and accounting costs and the licensing flexibility, the expected sales should be the deciding factor and not the law. Borloff demands that the right owner should be able to decide between a collecting society and self-management.

Elmar Hucko, Head of Departmental at the Federal Ministry of Justice, cut in on the discussion. His addition to the Ten Commandments was: “*No private copying without compensation*”. Therefore the collecting societies are in the right, especially when bearing in mind that CD-writers can produce “*copies of S-class quality*” (referring to the s-class cars of Daimler Chrysler). With the term “*S-class*” Hucko referred to the high quality of digital copies. But despite such “*unchastely*” devices the ICT industry still does not show much willingness to pay.

Reinbothe also talked about this problem. According to him the implementation is only possible when the technical devices for copy protection are fully functioning and accepted by the market and the users. Flat rate levies on blank medias or all kinds of copy devices would theoretically become unnecessary for the user gets the licences directly from the right owners. After a transitional period the national collective and flat rate remuneration systems should step aside for the widespread employment of DRM systems.

In his introductory lecture about the conversion of the EU Copyright Directive into German law Hoeren already referred to the conflict over the remuneration system for digital goods. He accused the music industry of double dealing. On the one hand it still charges remuneration flat rates for private copies on blank media and on the other hand it prevents private copies by means of DRM and copy protection systems. In the end the user is the one to suffer because he has to pay twice or he has to pay for something he can not use. Dr. Kathrin Bremer, legal advisor BITKOM, had similar arguments. Anke Schierenholz, corporate attorney Bild-Kunst (German collecting society) contradicted this. She did not see the existence of individual and flat rate remuneration as a way to “get paid twice” According to Nic Garnett, policy advisor at InterTrust Technologies, the claim for remuneration has to be considered in the discussion about the private copy but the question is if such remuneration systems are still necessary in addition to DRMS.

Dr. Tilo Gerlach, Managing Director of the Gesellschaft zur Verwertung von Leistungsrechten mbH (German collecting society) really brought the position of the panel of right owners to the point in saying: “*Protect things that can be protected and remunerate instead of give away things that can not be protected*”.

VI Final Result

At the beginning we pointed out that the second conference was organized to assess the current situation with regard to DRM. Naturally this can only be a snapshot. Because of the current state of flux this topic could not be brought to an end.

The conference helped to structure the topic. This book pursues the same objective. The anthology is based on the discussions at the conference and outlines in detail the technical, legal, economic and political aspects with regard to the employment of DRM systems.

VII Facts and Figures of the DRM Conference 2002

The second DRM conference took place on January 20th and 21st in the Haus der Wirtschaft (house of industry) in Berlin. The conference was organized by the Research Alliance Data Security North–Rhine Westphalia with its two sub-projects “Security for Digital Goods” (Universität Dortmund) and “Research Management” (Ruhr–Universität Bochum). The German Chamber of Industry and Commerce was co–organizer and the initiative media.nrw and the GITS AG (Company for IT Security Bochum) were cooperation partners.

The organizers were Prof. Eberhard Becker (Universität Dortmund, Conference Chair), Dr. Stefan Bechtold (Universität Tübingen), Dirk Günnewig (Universität Dortmund, Organisational Chair), Dr. Ina Pernice (DIHK) and Dr. Tomas Sander (at that time InterTrust StarLab). The conference office was situated in Bochum and Dortmund. The administrative employee Matthias Sassenberg and the student assistant Dietmar Palter worked there too. Several other people helped to make the conference a success. Here Petra Henseler has to be especially mentioned. She contributed essentially to the foundation of the research federation Datensicherheit Nordrhein–Westfalen (data security North–Rhine Westphalia) and without her commitment the project EURUBITS — Europäisches Institut für IT–Sicherheit (European Institute for IT Security) would not have been realized.²¹³⁴ Furthermore, we have to thank Marcus Heitmann, Ute Rode, Ulrike Schneider–Schleppe and Hellen Tackenberg (Universität Bochum) as well as Katrin Butzin, André Heymann, Dana Lange and Claudia Lorenz (DIHK) and Lorita Jahn (Universität Dortmund).

250 participants from science and practice and with a legal, economic or technical background took part in the two–day conference. The participants were representatives of the content industry, the ICT companies, the DRM producers, the collecting societies, political institutions and science. The organizers’ interdisciplinary demand was met with regard to programme and participants.

²¹³⁴ Meanwhile the institute includes a university institute with three chairs and one institute for further education.

The participants came from all over the world: from Germany, from other European countries, from Japan, from Korea and from the USA.

During the conference and at an evening event at the end of the first day the participants had the opportunity to talk to each other. At this evening event discussions took place in a relaxed atmosphere. They improved the networking. The venue of this event, the Berlin Meistersaal, is connected with the topic of the conference. The Meistersaal is a recording studio of the Hansa-Studios which have been built around the turn of the 19th century. Artists like U2, David Bowie and Johannes Hesters recorded their songs in this studios.

The lectures held at the conference can be downloaded from the conference website under the address <http://www.digital-rights-management.de> as an MP3-file (without DRM). At this site you can also find some of the slides presentations and other materials.

Acknowledgements

We like to thank Sylvia Ebbes (Universität Dortmund) and Dietmar Paltner (Ruhr-Universität Bochum) for their support in writing this article.

B Authors

Tobias Bauckhage, MEd

The Boston Consulting Group (BCG)

Tobias Bauckhage works for the Berlin office of The Boston Consulting Group (BCG), with a focus on telecommunication and the media industry. He holds a Master of Economics and Management Science of Humboldt University, Berlin and Carlos III, Madrid and prior to BCG has worked for different media companies.

Dr. Stefan Bechtold

J.S.M. (Stanford)

University of Tübingen Law School

Research Assistant, Chair of Prof. Dr. W. Möschel

stef@n-bechtold.com – <http://www.jura.uni-tuebingen.de/~s-bes1>

Stefan Bechtold studied law at the University of Tübingen Law School, Germany, from 1994 to 1999. In 1999 and 2000, he was a Visiting Scholar at the University of California at Berkeley School of Law. In 2001, he received a doctorate degree (Dr. iur.) from the University of Tübingen Law School. Supported by a Fulbright scholarship, he received a master's degree (J.S.M.) from Stanford Law School in summer 2002. From 2002 to 2003, he is a Fellow at the Center for Internet and Society at Stanford Law School. Since 1997, he has been working as a research assistant to Professor Dr. Wernhard Möschel at the University of Tübingen Law School. Mr. Bechtold is the author of numerous publications in the area of cyberlaw and intellectual property, including a 450 page book on the implications of digital rights management. Since 1997, he has been maintaining the Link Controversy Page, a web page on legal questions of hyperlinks, frames and inline images.

Rector Prof. Dr. Eberhard Becker (co-editor)

University of Dortmund, Professor of Mathematics

eberhard.becker@digital-rights-management.org

<http://www-lsii.mathematik.uni-dortmund.de>

Born 23.7.1943	in Stavenhagen, Germany
1964-1970	Studies of Mathematics and Physics (minor subject) at the University of Hamburg, Germany
1972	PhD in Mathematics at the University of Hamburg
1976	Habilitation in Mathematics at the University of Cologne
1979-	Full Professor for Mathematics, Chair for Algebra, at the University of Dortmund
1990-2001	Managing Editor of the “Mathematische Zeitschrift”, Editor of the Springer Series “Algorithms and Computations in Mathematics”
1998-2002	Member of the Research Alliance Data Security of North Rhine-Westphalia, Germany
2002-2006	Rector of the University of Dortmund

Peter Biddle

Microsoft Corporation; peterbi@microsoft.com

Peter Biddle runs Microsoft's Trusted Platforms Technologies Platform group, developing the Next Generation Secure Computing Base technologies and distributed trust architectures. Prior to this Peter was a Hardware Technical Evangelist focused on DVD, consumer technologies, and content protection, and was a founding participant in CPTWG and SDMI. Peter has worked for Microsoft since 1990 and has worked closely with the hardware industry since 1993.

Dr. Bettina Böhm

Universität Dortmund — Head of the Office of Academic and Student Affairs
Bettina.Boehm@uni-dortmund.de

Bettina Böhm was born in 1966 in Germany. After studying law at the Universität Bielefeld, she graduated in law in 1990 (First State Examination) and in 1994 (Second State Examination). After a short working stay at a law firm specialized in Copyright and Patent Law in Milan, Italy, she received a Doctoral Degree of the Universität Bielefeld, the doctoral thesis covering legal aspects of public private partnerships in regional development. Since 1996 she is Head of the Office of Academic and Student Affairs at the Universität Dortmund.

Oliver Bremer, MCS

Nokia

Is employed by Nokia as a technology specialist in the area of Digital Rights Management. A scholar of the German National Merit Foundation (Studienstiftung des deutschen Volkes), he graduated with a Masters degree in Computer Science from the University of Tulsa, U.S. During his Masters studies he held a research assistantship at the University's Center for Information Security and published numerous articles in the field of computer security.

Willms Buhse (co-editor)

Bertelsmann Digital World Services — Sr. Director Consulting
willms.buhse@digital-rights-managemnt.org

Willms Buhse holds a key role in both Digital World Services' formation and in the company's growing importance as a pioneer in the field of digital rights management (DRM) services. In various positions, incl. Head of Marketing, Business Development, Consulting and Product Management, he has worked with clients like ATT, BMG, HP, Lycos, Matsushita, Napster, Orange, Universal and holds the Vice Chair of the Open Mobile Alliance. He is also actively involved as an author and speaker on the subject of e/m-commerce in the media industry and for the EU Commission. He has been quoted in Billboard, Computerwoche, Frankfurter Allgemeine, Herald Tribune, Musicweek, Music & Copyright, Reuters, Spiegel, Webnoize, Zeit. Previously, he has worked for Roland Berger, Empresarios Agrupados and Reemtsma.

Dr. Lee A. Bygrave

B.A.(Hon.s)(A.N.U.), LL.B.(Hon.s)(A.N.U.), LL.D./dr. juris (Oslo)
 Norwegian Research Centre for Computers and Law - University of Oslo
 Senior Researcher
 lee.bygrave@jus.uio.no – <http://folk.uio.no/lee>

Is Senior Research Fellow at the Norwegian Research Centre for Computers and Law attached to the Law Faculty of the University of Oslo. He is also Barrister of the Supreme Court of New South Wales, Australia and former Co-Director (now Research Associate) of the Baker & McKenzie Cyberspace Law and Policy Centre at the University of New South Wales. His fields of speciality are privacy/data protection law, consumer protection law, information security, private international law and ADR/ODR. Amongst his publications are two books on data protection law, *Personvern i praksis* [Privacy and Data Protection in Practice] (Oslo, 1997) and *Data Protection Law: Approaching Its Rationale, Logic and Limits* (The Hague, 2002). He has written and lectured extensively on the interrelationship of copyright law and privacy/data protection law. His current work focuses on consumer protection issues in relation to e-commerce.

Spencer Cheng

Morphbius Inc. — Next generation multimedia technology
 spencer@morphbius.com

Spencer graduated with a B.Math (Honours, Computer Science) from the University of Waterloo (Waterloo, Canada) in 1983. After graduation, he worked at a variety of technology companies in the Ottawa area including Mitel, WebPlan, Bell-Northern Research/Nortel Networks (1990) and Cloakware (1998). Spencer developed the trust model for MPEG-4 IPMP.

At the present, Spencer is one of the founders of Morphbius Inc., a company that is developing next generation multimedia technology.

Dr. Michel Clement

Institute for Research in Innovation Management
 Christian-Albrechts-University of Kiel – Assistant Professor
 michel@michelclement.com – <http://www.michelclement.com>

Michel Clement was born on June 19th 1971 in Kiel, Germany. He is Dutch citizen and lives in Hamburg, Germany. Michel is researching media management and marketing with a current focus on movies and books. He published several books and articles about online media business. Michel has been three years with Bertelsmann in different management and consulting positions and founded a peer-to-peer-software company together with Bertelsmann Multimedia GmbH. He holds a doctoral and master's degree from the Institute for Research in Innovation Management, Christian-Albrechts-University of Kiel.

Prof. Dr. Thomas Dreier, M.C.J.

University of Karlsruhe
 Director, Institute for Information Law
 recht@ira.uka.de – <http://www.z-a-r.de>

Professor of Law at the University of Karlsruhe, Germany, where he is the Director of the Institute for Information Law, and Honorary Professor at the Law Faculty of the University of Freiburg. In spring 2002, Prof. Dreier was Global Visiting Professor of Law at the New York University, School of Law. Before joining the University of Karlsruhe, Prof. Dreier has been working at the Max-Planck-Institute for Foreign and International Patent, Copyright and Competition Law, Munich, Germany (1983 - 1999). Prof. Dreier is vice-president of the Association littéraire et artistique internationale (ALAI) and vice-chairman of ALAI's German national group as well as a Member of the Legal Advisory Board of the EU's DG Information Society and of the Advisory Panel on Intellectual Property of the Steering Committee of the Mass Media of the Council of Europe. Prof. Dreier also acts as Executive Secretary of the German Computer Law Society (Deutsche Gesellschaft für Recht und Informatik, DGRI). Major publications include "Rechts-Handbuch zum E-Commerce", 2001 (ed., with H.-W. Moritz); "Towards Consensus on the Electronic Use of Publications in Libraries-Strategy issues and recommendations", Göttingen 2001 (available at <http://www.sub.uni-goettingen.de/gdz/tecup/towacons.pdf>), and "Copyright Law and Digital Exploitation of Works - The Current Copyright Landscape in the Age of the Internet and Multimedia", Friedrich-Ebert-Foundation/International Publishers' Copyright Council, 1997.
 (http://www.ipa-uei.org/copyright/copyright_pub/dreier.html)

Séverine Dusollier

Centre de Recherches Informatique et Droit - University of Namur
 Senior Researcher
 severine.dusollier@fundp.ac.be

Séverine Dusollier has a Law Degree and is teaching copyright and cyberlaw at the University of Namur (Belgium). She is the Head of the IPR Department at the CRID (Research Centre for Computer Law) since 1998. She carried out research in several European and national projects and drafted reports for the WIPO, the Council of Europe, UNESCO and the European Commission. She is drafting a PhD about copyright and Digital Rights Management systems. She was a research associate at the University of California, Berkeley in 2001.

Paul England, Ph.D.

Microsoft Corporation; pengland@microsoft.com

Paul England is an architect in Microsoft's Trusted Platform Technologies group. He is developing hardware and software systems to increase data security in open systems like the PC. Prior to this he was in Microsoft Research where much of the technical work originated. Paul holds a Ph.D. in physics from Imperial College in London.

Marc Fetscherin

Institute of Information Systems - University of Bern
 Research and Teaching Assistant, PhD student
 fetscherin@iwi.unibe.ch

After studying management at the University of Lausanne (HEC) and his Masters degree in IT and Strategy at the London School of Economics (LSE), Marc Fetscherin worked as a consultant at McKinsey & Company where he got specialized in telecommunication and e-Commerce. Currently he is a research and teaching assistant at the Institute of Information Systems at the University of Bern, Switzerland. His research focuses on e-Commerce, Digital Content Distribution, and Digital Rights Management.

Dr. Marina Fiedler, MBR

Ludwig-Maximilians-Universität München, Munich School of Management.
 Research Associate at the Institute for Information, Organization and Management.
 fiedler@bwl.uni-muenchen.de – <http://www.iuk.bwl.uni-muenchen.de>

Marina Fiedler specializes in research on knowledge, openness, digitalisation and expertise. In addition to her MBR course she has taught the core courses Knowledge Management and Digitalisation, Production and Organization, Business Planning and Entrepreneurship, and Corporate Development. She earned her Ph.D. in Business Administration from Ludwig-Maximilians-Universität in Munich in 2003.

Dipl.-Inf. Robert A. Gehring

Technical University of Berlin – rag@cs.tu-berlin.de

Born in 1969, Robert A. Gehring studied electrical engineering, computer science and philosophy. He graduated with a Dipl.-Inform. degree from the Technical University of Berlin. As a member of the computers and society research group at the Technical University of Berlin his research is directed towards issues of internet governance, intellectual property rights, information security, and open source software. He is also a freelance consultant and has co-authored a variety of studies for the german federal government, e.g. an expertise on matters of software patents in 2000.

Dr. Bettina Goldmann, LL.M.

Baker & McKenzie
 Associate Attorney
 bettina.goldmann@bakernet.com

As an attorney with an international clientèle, Bettina Goldmann advises German and multinational companies in the field of computer and internet law, information technology, licensing and intellectual property law and above all in copyright law. Before joining Baker & McKenzie a couple of years ago, Bettina Goldmann worked as a research fellow at the Max Planck Institute for Foreign and International Patent, Copyright and Unfair Competition Law in Munich, where she also wrote her doctoral thesis on copyright and antitrust law dealing with the legal situation and practice of the copyright collecting societies in the US and Germany (Dr. jur., Munich, 2000). She graduated from New York University completing a Master of Laws Program (LL.M.) specialized in intellectual property law (1998) after having finished her legal studies in Germany (Freiburg, Munich) and in Grenoble/France (1988 - 1994) and having passed the Second State Examination. Bettina Goldmann regularly contributes to the

German and international legal press on topics regarding copyright law, intellectual property and computer law. Bettina Goldmann is located at the Munich office of Baker & McKenzie, but works during 2003 with Baker & McKenzie Paris and London.

Dirk Günnewig, MA (co-editor)

Research Assistant, Institut für Algebra und Geometrie, Universität Dortmund
 PhD Student, Sektion für Politikwissenschaften, Ruhr-Universität Bochum
 dirk.guennewig@digital-rights-management.org
 http://guennewig.digital-rights-management.de

Dirk is a Research Assistant working in the project “Digital Rights Management — Technological, Economic, Legal and Political Aspects” at the Institute of Algebra and Geometry at the University of Dortmund, Germany.

He has received an MA in Political Science from the University Münster, Germany and is currently working on his PhD thesis on “Regulation of DRM Systems” at the Section for Political Science at the University of Bochum, Germany.

His research focused on policy analysis, the analysis of political interests and lobbying, political regulation strategies, Digital Copyright, and Digital Rights Management.

Between 2000 and 2001, Dirk worked as a Research Assistant at the European Institute for IT-Security of the University of Bochum and in the Research Alliance IT-Security North-Rhine-Westphalia during which he co-organised two interdisciplinary DRM conferences held 2000 and 2002 in Berlin. In 2002 Dirk spent some time at the University of California at Berkeley as a Research Associate. Dirk is also a regular author for German computer and high-tech magazine, like *c't*.

Dipl.-Wirt. Inform. Susanne Guth

Vienna University of Economics and Business Administration
 Assistant Professor
 susanne.guth@wu-wien.ac.at

Susanne Guth received her degree in Information Systems from the University of Essen in Essen/Germany in 2000. She specialized in software techniques and production/operations management. Based on this work, she received a DAAD scholarship in 1997, and studied in the United States at Clemson University in Clemson, South Carolina.

Since August 2000, she has been an assistant professor in the Department of Information Systems at the University of Economics and Business Administration in Vienna, Austria. The Department has been recognized as pioneering the work in this field. For the last two and a half years, her research focus has been on contract and rights management for digital goods. She is writing her doctoral thesis in this field. Her latest publications address DRM frameworks and the enforceability of digital contracts.

Dr. Stuart Haber

Hewlett-Packard Labs, Princeton, New Jersey — stuart.haber@hp.com

Stuart Haber is a researcher at HP Labs. Along with Scott Stornetta, he was a co-founder of Surety, Inc., which was spun off by Bellcore in 1993 to commercialize the secure digital time-stamping technology that the two of them developed as researchers at Bellcore (now Telcordia Technologies). In addition to Bellcore and Surety, he has also worked as a researcher in STAR Lab, the research arm of InterTrust Technologies, the DRM provider. Haber received his B.A. from Harvard University and his M.S. from Stanford University, both in mathematics, and his Ph.D. in computer science from Columbia University in 1988. He has lectured and published on several practical and theoretical aspects of cryptography, on the theory of computing, and in electrical engineering.

Dr. Frank Hartung

Ericsson Research - Master Researcher
Frank.Hartung@ericsson.com

Frank Hartung is a Master Researcher with the Multimedia Technologies branch of Ericsson Research. He is the Ericsson representative in the DRM working group of the Open Mobile Alliance (OMA) standardization forum. Frank has several years of professional technical experience in the fields of DRM, mobile multimedia technology, multimedia security, and watermarking. He holds a M.Sc. from Aachen University of Technology and a Ph.D. from University of Erlangen, Germany, both in electrical engineering.

Tobias Hauser

Hauser & Wenz; Partner — <http://www.hauser-wenz.de/>

Tobias Hauser is a technical writer on various topics of computing and the Internet, something he started shortly after beginning his studies in business and administration at LMU Munich. He is working as an IT consultant and trainer and regularly writes articles for IT magazines. He lives in southern Germany.

Dr. Jürgen Herre

Fraunhofer Institut für Integrierte Schaltungen
 Chief Scientist, Audio/Visual

Jürgen Herre joined the Fraunhofer Institute for Integrated Circuits (IIS) in Erlangen, Germany, in 1989. Since then he has been involved in the development of perceptual coding algorithms for high quality audio, including the well-known ISO/MPEG-Audio Layer III coder (aka “MP3”).

In 1995, Dr. Herre joined Bell Laboratories for a PostDoc term working on the development of MPEG-2 Advanced Audio Coding (AAC). Since the end of '96 he is back at Fraunhofer working on the development of advanced multimedia technology including MPEG-4, MPEG-7 and secure delivery of audiovisual content, currently as the Chief Scientist for the Audio/Multimedia activities at Fraunhofer IIS, Erlangen.

Dr. Herre is a fellow of the Audio Engineering Society, co-chair of the AES Technical Committee on Coding of Audio Signals and vice chair of the AES Technical Council. He also served as an associate editor of the IEEE Transactions on Speech and Audio Processing and is a long time active member of the ISO/MPEG audio subgroup.

Prof. Dr. Thomas Hoeren

University of Münster (FRG) - Law Professor

Head of the Institute for Information, Telecommunication and Media Law (ITM) at the Faculty of Law

Head of the Research Center for Industrial Property Law

From 1 March 1996: Part Time Judge at the Court of Appeal of Düsseldorf (Copyright Senate)

Education:

- Summer Law School at the City of London Polytechnic (1983)
- Stagiaire at the Copyright Division of the UNESCO (1985)
- Doctorate in Canon Law (Lic. theol.), Faculty of Theology, University of Münster, FRG (1986)
- first State Examination in law (1987)
- Doctorate in Civil Law (Dr. iur., Ph. D.), Faculty of Law, University of Münster, FRG (1989)
- Second State Examination in law (1991)
- Habilitation in Civil Law (Dr. habil.), Faculty of Law, University of Münster, FRG (1994)

Honours:

- Member and Vice President of the German Association for Law and Informatics (DGRI)
- Member of the Society for Computers and Law (U.K.)
- Member of the German-Japanese Law Association (Hamburg/Tokyo)
- Co-editor of “Computer und Recht” (Computer and law/Cologne)
- Member of the Institute for European media law (Saarbrücken/FRG)
- Member of the Editorial Board of “Law, Computers and Artificial Intelligence”, the “BNA’s Electronic Information Policy & Law Report” and the “EDI Law Review”
- Legal adviser of the European Commission/DG XIII within the “Legal Advisory Board on Information Technology”
- Co-editor of “Multimedia und Recht” (Munich/FRG)
- Member of the Task Force Group on Intellectual Property Rights of the European Commission
- Legal expert in several research projects commissioned by the European Commission/DG III (COPEARMS), DG XIII (MULTISOLUTION, EDIBOL, EDIPAY) and the DG XV
- Member of the Legal Advisory Board of the DENIC (Frankfurt)

Dr. Bill Horne

Hewlett-Packard Labs, Princeton, New Jersey — whorne@hp.com

Dr. Bill Horne is a research scientist at Hewlett-Packard Labs in Princeton, New Jersey. He is a member of the Trusted Systems Lab at HP which conducts research in trust, security and privacy technologies. Before joining HP, he worked for STAR Lab, the research lab of InterTrust Technologies in Santa Clara, California on a broad range of topics relevant to advanced digital rights management (DRM). Bill Horne received a doctoral degree in Electrical Engineering from the University of New Mexico in 1993. From April 1993 to September 1996 he was a member of the research staff at NEC Research Institute in Princeton, New Jersey. His research interests include computer security including tamper resistant software and digital rights management.

Dirk Kuhlmann

Hewlett Packard Laboratories – Senior Research Engineer
derek@prz.tu-berlin.de

Dirk Kuhlmann received his degree in Computer Science from Technical University Berlin, and has been employed by Hewlett Packard Laboratories, Bristol, since 1995. Amongst others areas, he has worked on Realtime Systems, Electronic Publishing, and IT infrastructure for secure financial and business transactions. His current research focusses on hardware and software support for Platform Security. His particular interest are security architectures that are based on Open Source Software. This includes aspects of system design, development methodologies, evaluation and assurance, as well as economic, social and political impacts.

Dr. Mathias Lejeune

Mathias.Lejeune@t-online.de

Dr. Mathias Lejeune, attorney at law in Munich, Germany, is a member of the board of directors of the German Association of Law and Informatics (“DGRI”) and represents a major manufacturer of computer hardware products at BITKOM, the german IT industry trade representation in the discussion about DRM Systems and the introduction of levies on digital products such as PC Systems. Dr. Lejeune has many years of practical experience in negotiating IT contracts with major international, especially US companies. He is publisher and co- author of the book “Der E-Commerce-Vertrag nach amerikanischem Recht; der Uniform Computer Information Transaction Act (“UCITA”) und seine Auswirkungen auf die Praxis des Vertragsrechts”, Otto Schmidt Verlag, Köln 2001. Dr. Lejeune is member of the board of editors of the law magazine “Der IT Rechtsberater” and well known for his articles about international IT and contract law in various law magazines.

Georg Nolte

Institut for Information Law - University of Karlsruhe
Research Assistant
Georg.Nolte@web.de

Georg Nolte is born 1974 in Bochum, Germany. He Studied Law in Hamburg and Strasbourg. At present he works as an Assistant for Prof. Thomas Dreier at the Institut for Information Law in Karlsruhe and as a legal trainee in Hamburg.

Dr. Norman Paskin

The International DOI Foundation - Washington & Geneva

Dr. Norman Paskin became the first Director of The International DOI (Digital Object Identifier) Foundation in March 1998. Prior to this he worked for twenty years in the scientific publishing industry in both the U.S. and Europe, in roles including editorial, management, and information technology development. He was actively involved in information identifiers issues for the scientific technical and medical publishing community, and has published several papers on this and related topics.

The International DOI Foundation (<http://www.doi.org>) was established in 1998 to support the needs of the intellectual property community in the digital environment. The Foundation is supported by member organisations from a broad spread of interests such as technology companies, professional publishers.

Norman has led the DOI Foundation in its development of the DOI as a standardised identifier for the intellectual property communities (including text, music, images, and multimedia), which can work with existing identifiers and internet technology. He is actively involved with a range of related standards activities developments, and is responsible for the appointment of service providers for the efficient operation of the technology and business activities of the DOI system, and in engaging Foundation members in active involvement in defining policies and solutions.

For further information on the DOI initiative and the DOI Foundation, please see the DOI web site (www.doi.org).

DOI and DOI.ORG are registered trademarks of the International DOI Foundation.

Joe Pato

Hewlett-Packard Labs, Cambridge, Massachusetts — joe_pato@hp.com

http://www.hpl.hp.com/personal/Joe_Pato

Joe Pato is a Principal Scientist with the Trusted Systems Lab at HP Labs and is also the manager for the Trusted Systems Lab's Princeton research group. He has previously served as Chief Technology Officer for Hewlett-Packard's Internet Security Solutions Division. His ongoing research interest is in the technical and public policy aspects trust issues underlying effective collaboration environments. This interest has led him to look at preservation of internet communication in the event of cyber-terrorism; trust frameworks for mobile environments and how to apply privacy considerations in complex systems.

Marcus Peinado, Ph.D.

Microsoft Corporation; marcuspe@microsoft.com

Marcus Peinado is an architect in Microsoft's Trusted Platform Technologies group. Prior to joining Microsoft, he was a research scientist at the German National Research Center for Information Technology. His research interests include system security, cryptography and algorithms. Marcus holds a Ph.D. in computer science from Boston University and a Diplom-Informatiker degree from the Technical University of Berlin.

Dr. Fabien A. P. Petitcolas

Microsoft Research

Researcher

fabienpe@microsoft.com

Fabien Petitcolas received his PhD on "information hiding" in 1999 from the University of Cambridge, England. He then joined Microsoft Research as a researcher. He is the editor of the first book on information hiding. In 2002 he chaired the fifth international workshop on information hiding and the first international workshop on digital watermarking.

Prof. Dr. Dres. h.c. Arnold Picot

Ludwig-Maximilians-Universität München, Munich School of Management.

Head of the Institute for Information, Organization and Management.

picot@bwl.uni-muenchen.de – <http://www.iuk.bwl.uni-muenchen.de>

Arnold Picots research focuses on the interdependencies between information and communication technology and organizational structure. He has published numerous books

and papers dealing with organizational design, information and communication management and the evolution of new organizational forms, including topics such as office communication, electronic data interchange, telecommunication, electronic markets and virtual organizations. He has taught at universities in Germany, Switzerland (St. Gallen) and the United States (Stanford). His theoretical work is complemented by various research and consulting projects in the industry and the public sector. He holds several editorial positions and is a member of numerous boards including the German Federal Ministry for Research and Technology, the Regulatory Authority for Telecommunications and Posts, the Munich Circle — Supranational Association for Communications Research (Münchner Kreis), as well as of several boards of directors and advisory bodies.

Avni Rambhia, MS

Eyemail Technology, Inc. - Video technology development
a_rambhia@yahoo.com – <http://paul.rutgers.edu/~sharahul/avni>

Avni Rambhia is a video and image technology expert with special interest in multimedia security. As a core MPEG-4 technology developer at e-View, she developed, designed and managed a suite of MPEG-4 image codecs and related applications, and created patent-pending multimedia security technologies. Avni is one of the key architects of the MPEG IPMP Extensions specification, and served as its editor for the year 2000-01. She currently serves as a technology consultant to Eyemail Technology, Inc., and as an advisor to Morphbius, Inc. She earned her Master's degree in Electrical Engineering at the University of Washington, Seattle, in 1999.

Prof. Dr. Jörg Reinbothe

Professor (Saarland University, Europa-Institut), Dr. jur., M.C.L. (University of Michigan); Head of Unit "Copyright and Neighbouring Rights" in Directorate General Internal Market of the European Commission, Brussels.

Legal Studies at Universities of Freiburg and Munich (Germany), Lausanne (Switzerland) und Ann Arbor (Michigan, USA).

From 1978 to 1986 Federal Ministry of Justice, Bonn. Main activities in the areas copyright, unfair competition, industrial property, and international aspects of intellectual property. For three years spokesman of the Ministry and deputy head of the public relations unit.

From 1986 to 1988 Legal Counsellor in the Permanent Representation of the Federal Republic of Germany to the United Nations in New York (USA). 1988 entry into the European Commission (Directorate General III, Internal Market and Industrial Affairs). Main activities: negotiations on the TRIPs Agreement for the protection of intellectual and industrial property in the GATT/Uruguay Round; EC Directive on rental and lending rights.

Since 1990 teaching intellectual property at the Saarbrücken University (Europa-Institut); Professor since 2003. Author/co-author of numerous articles and 3 books. From 1993 to 1996 Assistant to the Director General of DG XV (Internal Market and Financial Services).

Since 1996 Head of Unit DG Internal Market/E-3 (Copyright and Neighbouring Rights). Head of the EC delegation at the WIPO Diplomatic Conferences of 1996 and 2000.

Niels Rump (co-editor)

Senior Consultant, Rightscom Ltd. — niels.rump@digital-rights-management.org

Niels has over seven years experience in DRM-related industries. In the 1990s, Niels began working on developing tools to manage and protect content related intellectual property rights while working at the Fraunhofer Institute for Integrated Circuits in Erlangen, Germany. He is one of the main developers of Fraunhofer's Multimedia Protection Protocol (MMP) and his name is assigned to several German and international patents related to this work.

Since 1997, he has been chairman of various task groups on Intellectual Property Management & Protection (IPMP) of MPEG. Niels was also secretary of the Audio Engineering Society's standards committee on Internet Music Delivery Systems and chairman of the Functional Requirements Working Group of the Secure Digital Music Initiative (SDMI). In 2002, he has been awarded an "ISO/IEC Certificate of Appreciation" for his work on MPEG-4 IPMP. More recently, Niels worked for InterTrust Technologies International as Manager, Standards & Multimedia, before joining Rightscom Limited as Senior Consultant in June 2001.

Niels holds a Diploma in Computer Science (approx. M.Sc.) from Erlangen University, Germany. He has published several articles about DRM issues and is a frequent contributor to topical conferences. He lives and works in London.

Dr. Ahmad-Reza Sadeghi

Saarland University, Computer Science
Im Stadtwald 45, D-66123 Saarbrücken, Germany
sadeghi@cs.uni-saarland.de

Ahmad-Reza Sadeghi is a member of research staff at the *Institute for Cryptography and Security*, department of *Computer Science* at *Saarland University*. His research interests are cryptographic protocols for electronic marketplaces and digital rights management systems.

Dr. Tomas Sander

Hewlett Packard Labs, Princeton, New Jersey

Dr. Tomas Sander is a research scientist at Hewlett Packard Labs in Princeton, New Jersey. He is a member of the Trusted Systems Lab at HP which conducts research in trust, security and privacy technologies. Before joining HP, he worked for STAR Lab, the research lab of InterTrust Technologies in Santa Clara, California on a broad range of topics relevant to advanced digital rights management (DRM). Tomas Sander received a doctoral degree in Mathematics from the University of Dortmund, Germany in 1996. From September 1996 to September 1999 he was a postdoctoral researcher at the International Computer Science Institute in Berkeley, California. He founded the ACM DRM Workshop in 2001. His research interests include cryptography, computer security, electronic commerce and digital rights management.

Dr. Markus Schneider

Fraunhofer Gesellschaft, Institute for Secure Telecooperation
 Dolivostraße 15, D-64293 Darmstadt, Germany
 markus.schneider@sit.fhg.de

Markus Schneider obtained both his diploma and Ph.D degree in Electrical Engineering. Currently, he is with the *Fraunhofer Institute for Secure Telecooperation* (FhI-SIT), department *Marketplace Internet*, in Darmstadt (Germany) as a postdoctoral researcher. His research interests include security and privacy issues in electronic business processes.

Dr. Barbara Simons

U.S. Public Policy Committee of the Association for Computing Machinery (USACM); founder and co-chair — Work with colleagues to select technology policy issues and positions for USACM
 simons@acm.org

Barbara Simons was President of the Association for Computing Machinery (ACM) from July 1998 until June 2000; in 1993 she founded ACM's US Public Policy Committee (USACM), which she currently co-chairs. Simons is a Fellow of ACM and the American Association for the Advancement of Science. She received the Alumnus of the Year Award from the U.C. Berkeley Computer Science Department, the Norbert Wiener Award from CPSR, the Outstanding Contribution Award from ACM, and the Pioneer Award from EFF. She was selected by c|net as one of its 26 Internet "Visionaries" and by Open Computing as one of the "Top 100 Women in Computing". Science Magazine featured her in a special edition on women in science. Simons served on the (U.S.) President's Export Council's Subcommittee on Encryption and on the Information Technology-Sector of the resident's Council on the Year 2000 Conversion. She is on the Board of Directors of the U.C. Berkeley Engineering Fund, Public Knowledge, the Math/Science Network, and the Electronic Privacy Information Center, as well as the Advisory Boards of the Oxford Internet Institute, the Public Interest Registry's .ORG and Zeroknowledge. She has testified before both the U.S. and the California legislatures and at government sponsored hearings. She was runner-up in the first election for the North America seat on the ICANN Board.

Dipl.-Math. Gabriele Spenger

Chair of Information Technologies with Focus on Communication Electronics at Friedrich-Alexander University Erlangen
 Postgraduate
 spenger@like.e-technik.uni-erlangen.de

- In 1998 Diploma in Mathematics at the Friedrich-Alexander-University Erlangen.
- In 1998-2001 at Fraunhofer Insitute for Integrated Circuits. I joined the Audio Department and worked in the area of cryptography, Digital Rights Management, MPEG-21 and MPEG-4 IPMP.
- In 2001 at the Friedrich-Alexander-University Erlangen. I am currently working towards my PhD degree in the area of security aspects of radio-frequency-identification-cards.

Robert E. Tarjan

James S. McDonnell Distinguished

University Professor at the Department of Computer Science, Princeton University
Office of Strategy and Technology, Hewlett-Packard
ret@cs.princeton.edu

Robert E. Tarjan is the James S. McDonnell Distinguished University Professor of Computer Science at Princeton University, and Chief Scientist at Hewlett-Packard. Prof. Tarjan is a world expert in the design and analysis of computer algorithms. He is the inventor or co-inventor of the most efficient known algorithms and data structures for problems in a wide variety of application areas. He has published over 170 refereed journal articles and book chapters. A member of the National Academy of Sciences, the National Academy of Engineering, and other learned societies, he was awarded the first Nevanlinna Prize in Information Science in 1983 and the Turing Award in 1986. Prof. Tarjan received his B.S. in mathematics from the California Institute of Technology in 1969 and his M.S and Ph.D. in Computer Science from Stanford in 1971 and 1972, respectively.

Dr. Johannes Ulbricht

ulbricht@michow-rechtsanwaelte.de

Dr. Johannes Ulbricht reads law and cultural management in Hamburg. During his studies, he worked for media lawyer and current constitution judge Prof. Hoffmann-Riem on copyright questions thrown up by the first DRM prototypes (CITED, Xanadu). As CEO of the Rudolf-Arnheim Institute for Art and Cultural Economy he is especially interested in the areas of conflict between technology, economy and art. In addition, Dr. Ulbricht is active in a music and media law practice and legal adviser to the Bundesverband der Veranstaltungswirtschaft (IDKV). He has published several articles on the subject of copyright and IT and on the whole area of DRM in legal journals and magazines of the entertainment industry. His cross-discipline dissertation also combines the economic, technical and legal aspects of DRM. He has also acted as a consultant to the DRM provider Bertelsmann Digital World Services.

Dr. Constanze Ulmer-Eilfort

Baker & McKenzie

constanze.ulmer-eilfort@bakernet.com

Constanze Ulmer-Eilfort is an International Partner of Baker & McKenzie Frankfurt office.

She studied at the University of Regensburg Law School (until 1984), Ludwig Maximilian Universität München Law School (first State Examination in 1987) and University of Pennsylvania Law School (LL.M. in 1989). Second State Examination, Bavaria, 1993. Dr. jur., Freie Universität Berlin, 1993. Admitted as attorney at law in New York (1990) and in Frankfurt (1993).

In 1994, she joined Baker & McKenzie as an associate, became Partner in 1998 and International Partner in 2000. She specializes in copyright law, publishing and media law, computer law, licensing and technology transfer agreements.

Constanze Ulmer-Eilfort is an active member of the German and European IP / IT Practice Groups of Baker & McKenzie. She is an expert in copyright and focuses on the protection and licensing of content and technology including their use via the Internet. She advises clients from the IT, telecommunications, technology and media industries.

Christian Wenz

Hauser & Wenz; Partner — <http://www.hauser-wenz.de/>

Christian Wenz started writing books on IT topics during his first term of studying computer science at TU Munich and has since then become author or co-author of over 30 books. Apart from that, he is frequently contributing to IT magazines and speaking at national and international conferences. He lives and works in Munich.

Amélie Wetzel

VIVICO REAL ESTATE GmbH, Frankfurt/Main

Education

- | | |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2000 – 2003 | OTTO-FRIEDRICH-UNIVERSITY, Bamberg, Germany
Doktorarbeit (PhD) in Human Resorce Management: Thesis on new business models for immaterial goods. Effects of the digitalization. |
| 1993 – 1998 | OTTO-FRIEDRICH-UNIVERSITY, Bamberg, Germany
Diploma in Business Administration. Majors in Human Resource Management and Organisation, European Community Law, Marketing.
Overall grade: 2.5 |
| 1992 | Abitur (roughly equivalent to A levels) |
| 1983 – 1992 | Max-Josef-Stift, Munich, Germany |

Work Experience

- | | |
|-------------|-------------------------------------------------------------------------------|
| Since 2003 | VIVICO REAL ESTATE GmbH, Frankfurt/Main
Corporate development and strategy |
| 2000 – 2003 | AUSSEM Haus + Grund, Munich
Assistant to the Management |
| 1999 – 2000 | BOELL CONCEPT GmbH, Munich
Assistant to the Management |

Prof. Rolf T. Wigand

University of Arkansas at Little Rock

Maulden-Entergy Chair and Distinguished Professor of Information Science and Management

Rolf T. Wigand is the Maulden-Entergy Chair and Distinguished Professor of Information Science and Management at the University of Arkansas at Little Rock. Rolf is the immediate past Director of the Center for Digital Commerce and the Master's and Graduate Program in Information Management, both in the School of Information Studies at Syracuse University. He is an internationally known researcher, consultant and speaker in information management, electronic commerce, and the strategic deployment of information and communication technology. His research interests lie at the intersection of information and communication business issues, the role of newer information technologies and their strategic alignment within business and industry. Wigand has taught on the faculty of Syracuse University, Stuttgart Institute for Information Management, Arizona State University, Michigan State University, Universidad Iberoamericana, Mexico City; and the University of Munich. Some of his research has been supported by the National Science Foundation, the Volkswagen Foundation, the International Social Science Council, Rome Laboratory, and other funding agencies. He has consulted for IBM, ALCATEL, Corning, Siemens AG, MITI-Japan, Rockwell

International, AT&T, Honeywell, U-HAUL International, Equitable General Insurance Company, Motorola, Anderson Clayton, Ford World Headquarters, Chase Manhattan Bank, Herman Miller, Banco Nacional de México, and others.

He holds several editorial positions with such journals as *The Information Society*, *Electronic Markets*, *Communications of the Association of Information Systems*, *Journal of Internet Banking and Commerce*, *Technology Studies*, *Telecommunications Policy*, *Journal of Technology Transfer*, *Communications: European Journal of Communication Research*, *Journal of Communication and Transnational Data and Communications Report*. He is an editorial board and review board member of almost 30 academic and professional journals, book series and yearbooks. Wigand is the author of four books and over 100 articles, book chapters, and monographs. His most recent book (with co-authors) is *Information Organization and Management: Expanding Markets and Corporate Boundaries*. This book has been translated into German and Japanese.

Bryan Willman

Microsoft Corporation; bryanwi@microsoft.com

Bryan Willman is an Architect in the Microsoft Windows Base team, and has spent the last few years developing some of the key technologies of Microsoft's Next Generation Secure Computing Base initiative. He has worked in the core OS group at Microsoft since 1984, in a broad range of OS and OS to hardware interface efforts.

C References

— A —

Abrazhevich (2001a)

Abrazhevich, D. (2001): Classification and characteristics of electronic payment systems. In: Electronic Commerce and Web Technologies. Second International Conference (EC-Web 2001).

Abrazhevich (2001b)

Abrazhevich, D. (2001): Electronic payment systems: Issues of user acceptance. In: eBusiness and eWork. Proceedings.

Abrazhevich (2001c)

Abrazhevich, D. (2001): A survey of user attitudes towards electronic payment systems. In: Conference on Human-Computer Interaction (HCI 2001), Proceedings.

Achilles, Schäfer, VUD (2001)

Achilles, Hermann/ Schäfer, Ronald/ Verband der Unterhaltungssoftware Deutschland (VUD) (30.8.2001): Richtlinie 2001/29/EG des europäischen Parlaments und des Rates zur Harmonisierung bestimmter Aspekte des Urheberrechtes und der verwandten Schutzrechte in der Informationsgesellschaft. Brief der Geschäftsführung des VUD an Dr. Irene Pakuscher vom Bundesministerium der Justiz. Berlin.

Adar, Huberman (2000)

Adar, E./ Huberman, B. (2000): Free riding on Gnutella. Technical report. Xerox-PARC.

Ahrens et.al. (2002)

Ahrens et.al. (eds.)(2002): Festschrift Erdmann. Cologne.

Aiello, Chung, Lu (2001)

Aiello, W./ Chung, F./ Lu, L. (2001): Random evolution in massive graphs. In: Proceedings of the 42nd Annual IEEE Symposium on Foundations of Computer Science. 510-519

Äijö, Saarinen (2001)

Äijö, T./ Saarinen, K. (2001): Business Models — Conceptual analysis. Available at: http://www.tbrc.fi/pubfile/TBRC_10042.pdf. Accessed: 4.7.2002.

Albers, Clement, Skiera (1999)

Albers, S./ Clement, M./ Skiera, B. (1999): Wie sollen die Produkte vertrieben werden? — Distributionspolitik. In: Albers, S./ Clement, M. et.al. (eds.)(1999): E-Commerce — Einstieg, Strategie und Umsetzung im Unternehmen. Frankfurt. pp. 79-94.

Albert, Jeong, Barabási (1999)

Albert, R./ Jeong, H./ Barabási, A.L. (1999): Diameter of the world-wide web. Nature 401. 130-131

Allamanche, Herre, Hellmuth, Fröba, Cremer (2001)

Allamanche, E./ Herre, J./ Hellmuth, O./ Fröba, B./ Cremer, M. (2001): "AudioID: Towards Content-Based Identification of Audio Material". 110th AES Convention. Amsterdam. Preprint 5380.

Ambikairajah, Davis, Wong (1997)

Ambikairajah, Eliathamby/ Davis, Andrew G./ Wong, W. T. Kenneth (August 1997): Auditory masking and MPEG-1 audio compression. *I.E.E. Electronics Communication Engineering Journal*. Vol. 9. No. 4. pp. 165–175.

Amit, Zott (2000)

Amit, R./ Zott, Chr. (2000): Value drivers of E-commerce business models. Papers presented at the 20th annual international conference of the Strategic Management Society. October 15–18 2000. Vancouver, British Columbia.

Anderson (1998)

Anderson, M.M. (1998): The electronic check architecture. Version 1.0.2. White Paper. Financial Services Technology Consortium (FSTC). Available at: www.echeck.org. September 1998.

Anderson (2001)

Anderson, Ross J. (2001): *Security Engineering — A Guide to Building Dependable Distributed Systems*. New York.

Anderson (2002)

Anderson, Ross J. (2002): Security in Open versus Closed Systems — The Dance of Boltzmann, Coase and Moore. Available at: <http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/toulouse.pdf>.

Anderson (2003)

Anderson, Ross J. (2003): TCPA/Palladium Frequently Asked Questions. Version 1.0. Available at: <http://www.cl.cam.ac.uk/~rja14/tpa-faq.html> (last modified Apr. 2003).

Anderson (2003a)

Anderson, Ross J. (2003): Cryptography and Competition Policy — Issues with “Trusted Computing”. Available at: <http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/tpa.pdf> (May 2003).

Anderson Consulting (2000)

Anderson Consulting (22.3.2000): A Bright Future for eBook Publishing: Facilitated Open Standards. AAP Annual Meeting. Available at: <http://www.publishers.org/digital/dec2000anderson.ppt>.

Anderson, Kuhn (1996)

Anderson, Ross/ Kuhn, Markus (1996): Tamper Resistance — A Cautionary Note. In: *The Second USENIX Workshop on Electronic Commerce Proceedings*. pp. 1–11. Available at: <http://www.ccl.cam.ac.uk/ftp/users/rja14/tamper.html> Last visited: 28 August 2001.

Anderson, Kuhn (1997)

Anderson, Ross/ Kuhn, Markus (1997): Low Cost Attacks on Tamper Resistant Devices. In: *Security Protocols. 5th International Workshop*. Paris, France. April 1997. Proceedings. pp. 125–136.

Anderson, Manifavas, Sutherland (1997)

Anderson, R./ Manifavas, C./ Sutherland, C. (1997): NetCard – A Practical Electronic Cash System. In: *Security Protocols. International Workshop 1996. Proceedings*.

Anderson, Stajano, Lee (2001)

Anderson, Ross/ Stajano, Frank/ Lee, Jong-Hyeon (2001): Security Policies. In: *Advances in Computers*. 55. pp. 185–235.

Andreoni (1988)

Andreoni, James (1988): Privately provided public goods in a large economy: the limits of altruism. In: *Journal of Public Economics*. 35. 1/1988. pp. 57–73.

Andreoni (1990)

Andreoni, James (1990): Impure altruism and donations to public goods: a theory of warm-glow giving. In: *The Economic Journal*. 100. June/1990. pp. 464–477.

Andres (2002)

Andres, R. (2002): *The European Software Piracy: An Empirical Application*.

Anonymous (2002)

Anonymous (April 2002): IEEE forbids papers violating DMCA. In: *NewsForge* (14.4.2002). Available at: <http://newsvac.newsforge.com/article.pl?sid=02/04/14/0039211>. last visited: 14.4.2002.

ANSI/NISO (2000).

ANSI/NISO Z39.84 – 2000 Syntax for The Digital Object Identifier. Available at: http://www.niso.org/standards/standard_detail.cfm?std_id=480.

Aoki (1993)

Aoki, Keith (1993): Authors, Inventors and Trademark Owners: Private Intellectual Property and the Public Domain. In: *Columbia-VLA Journal of Law and the Arts* 18.

Appel, Felten (1999)

Appel, Andrew W./ Felten, Edward W. (November 1999): Proof-Carrying Authentication. *Proceedings of 6th ACM Conference on Computer and Communications Security*.

Arbaugh (2002)

Arbaugh, William A. (2002): Improving the TCPA Specification. In: *IEEE Computer*, No. 8. Vol. 35. pp. 77–79.

Arbaugh, Farber, Smith (1997)

Arbaugh, William A./ Farber, David J./ Smith, Jonathan M. (1997): A Secure and Reliable Bootstrap Architecture. In: *IEEE Symposium on Security and Privacy*. *Proceedings*. pp. 65–71. Available at: <http://www.computer.org/proceedings/sp/7828/78280065.pdf>. Last visited: 28.3.2003.

ARD, ZDF (19.4.2002)

Stellungnahme der ARD und des ZDF zum Referentenentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft. Köln, Mainz.

Arrow (1962)

Arrow, Kenneth J. (1962): Economic welfare and the allocation of resources for invention. In: Nelson, R. (ed.): *The rate and direction of inventive activity: economic and social factors — A conference of the Universities-national bureau committee for economic research and the committee on economic growth of the social science research council*. Princeton, N.J. pp. 609–625.

Asay (2002)

Asay, Matt (Apr. 2002): A Funny Thing Happened on the Way to the Market: Linux, the General Public License, and a New Model for Software Innovation. Available at: <http://www.linuxdevices.com/files/misc/asay-paper.pdf>.

- Asokan, Janson, Steiner, Waidner (1996)
 Asokan, N./Janson, Phil/Steiner, Michael/Waidner, Michael (1996): Research Report RZ 2890 (# 90838): Electronic Payment Systems. IBM Research.
- Asokan, Janson, Steiner, Waidner (1997)
 Asokan, N./ Janson, P./ Steiner, M./ Waidner, M. (1997): The state of the art in electronic payment systems. In: IEEE Computer. 30(9). September 1997.
- Asokan, Janson, Steiner, Waidner (2000)
 Asokan, N./ Janson, P./ Steiner, M./ Waidner, M. (2000): The state of the art in electronic payment systems. In: Advances in Computers. 53. 2000.
- Aucsmith (1996)
 Aucsmith, D. (1996): Tamper-resistant software: An implementation. In: Anderson, R., ed.: Information hiding: first international workshop. Cambridge. U.K. Vol. 1174 of Lecture Notes in Computer Science. Springer-Verlag. pp. 317–333.
- Aucsmith (1998)
 Aucsmith, D. (ed.)(1998): Proceedings of the second international workshop on information hiding. Portland, Oregon, U.S.A. April 1998.
- Auer-Reinsdorff, Brandenburg (2003)
 Auer-Reinsdorff, Astrid/ Brandenburg, Andrea (2003): Urheberrecht und Multimedia. Berlin.
- B —
- Bakos, Brynjolfsson (1999)
 Bakos, Y./ Brynjolfsson, E. (1999): Bundling Information Goods: Pricing, Profits and Efficiency. Working Paper.
- Bakos, Brynjolfsson, Lichtman (1999)
 Bakos, Yannis/ Brynjolfsson, Erik/ Lichtman, Douglas (1999): Shared Information Goods. In: Journal of Law and Economics – Vol. 42 (1). April 1999. pp. 117–155.
- Bao, Deng, Han, Jeng, Narasimhalu, Ngair (1997)
 Bao, Feng/ Deng, Robert H./ Han, Yong F./ Jeng, Albert B.R./ Narasimhalu, Arcot D./ Ngair, Teow H. (1997): Breaking Public Key Cryptosystems on Tamper Resistant Devices in the Presence of Transient Faults. In: Security Protocols. 5th International Workshop. Paris, France. April 1997. Proceedings. pp. 115–124.
- Bappert (1957)
 Bappert, Walter (1957): Wege zum Urheberrecht. Die geschichtliche Entwicklung des deutschen Urheberrechts. Göttingen.
- Bär, Hoffmann (2002)
 Bär, Wolfgang/ Hoffmann, Helmut (2002): Das Zugangskontrolldiensteschutz-Gesetz — Ein erster Schritt auf dem richtigen Weg. In: MMR 2002. p. 654.
- Barabási, Albert (1999)
 Barabási, A.L./ Albert, R. (1999): Emergence of scaling in random networks. Science 286. pp. 509–512

- Barak et al. (2001)
 Barak, Boaz/ Goldreich, Oded/ Impagliazzo, Russel/ Rudich, Steven/ Sahai, Amit/ Vadhan, Salil/ Yang, Ke (2001): On the (Im)possibility of Obfuscating Programs. In: Joe Kilian (ed.): *Advances in Cryptology — CRYPTO 2001*. Berlin. p. 1.
- Barlow (1994)
 Barlow, John Perry (1994): The Economy of Ideas. In: WIRED. 2.03 March/1994. Available at:
<http://www.wired.com/wired/archive/2.03/economy.ideas.html>
- Barlow (1996)
 Barlow, John Perry (1996): Selling Wine without Bottles — The Economy of Mind and the Global Net. In: Hugenholtz (1996): p. 169.
- Barlow (2000)
 Barlow, John Perry (2000): The Next Economy of Ideas: Will copyright survive the Napster bomb? In: WIRED 8.10,240. Oktober 2000. Available at:
<http://www.wired.com/wired/archive/8.10/download.html>
- Barni, Bartolini, Cappellini, Piva (1998)
 Barni, Mauro/ Bartolini, Franco/ Cappellini, Vito/ Piva, Alessandro (May 1998): A D.C.T.-domain system for robust image watermarking. In: *Signal processing*. Vol. 66. No. 3. pp. 357–372.
- Bartel (2002)
 Bartel, M./ et. al. (Februar 2002): XML–Signature Syntax and Processing. W3C Recommendation. RFC 3275. Available at: <http://www.w3.org/TR/xmlsig-core/>.
- Bartholomew (2002)
 Bartholomew, Paul (July 14, 2002): Understanding the Xbox Boot Process/Flash Structures. Available at:
http://xbox-linux.sourceforge.net/articles.php?aid=2002_194020413.
- Barzel (1968)
 Barzel, Yoram (1968): Optimal Timing of Innovations. In: *Review of Economics and Statistics*. 50. pp. 348–355.
- Bass (1969)
 Bass, F. M. (1969): A New Product Growth Model for Consumer Durables, *Management Science*. 15. pp. 215–227.
- Bauckhage (2002)
 Bauckhage, Tobias (2002): Das Ende vom Lied? Zum Einfluss der Digitalisierung auf die international Musikindustrie. Stuttgart.
- BDB, DBV, DGI (2002)
 Bundesvereinigung Deutscher Bibliotheksverbände e.V., Deutschen Bibliotheksverband e.V., Deutsche Gesellschaft für Informationswissenschaft und Informationspraxis e.V. (6.9.2002): Gemeinsame Erklärung zum Regierungsentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft. Last visited: 12.12.2002. Available at:
http://www.urheberrecht.org/topic/Info-RiLi/st/ Gemeins_Erkl.pdf

BDI (2002)

Bundesverband der Deutschen Industrie (17.6.2002): Referentenentwurf für ein Umsetzungsgesetz zur Richtlinie Urheberrecht in der Informationsgesellschaft. Last visited: 17.6.2002. Available at: <http://www.bdi-online.de>

BDI (2000a)

Bundesverband der Deutschen Industrie (7.9.2000): PC-Abgaben der Bundesregierung verzerren den Wettbewerb. Pressemitteilung. Last visited: 24.4.2002. Available at: <http://www.bdi-online.de>

BDI (2002)

Bundesverband der Deutschen Industrie (3.2002): Stellungnahme. In: CDU/CSU-Bundestagsfraktion (2002): pp. 109–111.

BDI (2002a)

Bundesverband der Deutschen Industrie (19.4.2002): Stellungnahme zum Referentenentwurf für ein Umsetzungsgesetz zur Richtlinie Urheberrecht in der Informationsgesellschaft. Berlin. Last visited: 19.4.2002. Available at: <http://www.bdi-online.de>

BDI (2002b)

Bundesverband der Deutschen Industrie (19.4.2002a): Stellungnahme zum Referentenentwurf für ein Umsetzungsgesetz zur Richtlinie Urheberrecht in der Informationsgesellschaft. Brief von Dr. Kretschmer und Dr. Vieregge (BDI) an Dr. Irena Pakuscher(BMJ). Berlin. [Vom BDI zur Verfügung gestellt.

BDI (2002c)

Bundesverband der Deutschen Industrie (17.6.2002): Referentenentwurf für ein Umsetzungsgesetz zur Richtlinie Urheberrecht in der Informationsgesellschaft. Last visited: 17.6.2002. Available at: <http://www.bdi-online.de>

BDZV (2001)

Bundesverband Deutscher Zeitungsverleger (28.8.2001): Anmerkungen des Bundesverbandes Deutscher Zeitungsverleger e. V. (BDZV) zur Umsetzung der Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft (EU-Urheberrechtsrichtlinie). Last visited: 28.8.2001. Available at: ftp://ftp.rga.de/bdzbv/medpoli/bdzbvstellgn_eu_urheberrecht.zip

BDZV (2002)

Bundesverband Deutscher Zeitungsverleger (18.4.2002): Stellungnahme des Bundesverbandes Deutscher Zeitungsverleger e.V. (BDZV) zum Referentenentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft. Berlin.

Bechtold (1998)

Bechtold, Stefan (1998): Multimedia und Urheberrecht — einige grundsätzliche Anmerkungen. In: GRUR 1998, 19–27.

Bechtold (2002)

Bechtold, Stefan (2002): Vom Urheber– zum Informationsrecht — Implikationen des Digital Rights Management. Munich.

Bechtold (2002a)

Bechtold, Stefan (2002): The Problems of Perfection. Review of Cass Sunstein, Republic.com. In: 3 European Business Organization Law Review 237.

Bechtold (2003a)

Bechtold, Stefan (2003): Digital Rights Management in the United States and Europe. Unpublished draft.

Bechtold (2003b)

Bechtold, Stefan (2003): Governance in Namespaces. 36 *Loyola of Los Angeles Law Review* 1239.

Becker (1994)

Becker, Jürgen (1994): Die digitale Verwertung von Musikwerken aus der Sicht der Musikurheber. In: Becker, Dreier (1994): pp. 45–76.

Becker (1999)

Becker, Jürgen (1999): Konsequenzen für die Verwertungsgesellschaften und deren Lizenzierungssystem. In: Prütting, Hanns / Reinbothe, Jörg / Schöfisch, Volker / et.al. (ed.)(1999): Die Entwicklung des Urheberrechts im europäischen Rahmen. Expertentagung des Instituts für Rundfunkrecht an der Universität zu Köln am 2. und 3. Oktober 1998 in Köln. Schriftenreihe des Instituts für Rundfunkrecht an der Universität Köln. Band 75. München. pp. 53–71.

Becker (2000)

Becker, Jürgen (2000): Bewertung der Richtlinienentwürfe der EU aus der Sicht der Urheber und der Verwertungsgesellschaften. In: Schwarze, Jürgen (2000): Rechtsschutz gegen Urheberrechtsverletzung und Wettbewerbsverstöße in grenzüberschreitenden Medien. Baden-Baden. pp. 29–51.

Becker (2002)

Becker, Jürgen (30.1.2002): Die Rolle der Verwertungsgesellschaften im digitalen Zeitalter. Abstrakt zum Vortrag am 30.1.2002 auf der II. Digital Rights Management Konferenz am 29. und 30.1.2002 des Forschungsverbunds Datensicherheit im Haus der Wirtschaft. Berlin. Last visited: 30.1.2002. Available at: <http://www.digital-rights-management.de/digi/konferenzen/drm2002/programm/abstract/becker.htm>

Becker (2002a)

Becker, Jürgen (3.2002): Beiträge im Wortprotokoll der Anhörung vom 16.11.2000. In: CDU/CSU-Bundestagsfraktion (2002): pp. 157, 158, 159–160, 164.

Becker, Dreier (1994)

Becker, Jürgen / Dreier, Thomas (1994): Urheberrecht und digitale Technologie: Arbeitssitzung des Instituts für Urheber- und Medienrecht am 22. April.1994. Baden-Baden.

Becker, Ziegler (2000)

Becker, A./ Ziegler, M. (2000): Wanted: A survival plan for the music industry — Napster and the consequences. Diebold.

Beger (2002)

Beger, Gabriele (1.10.2002): Entwurf eines Gesetzes zur Regelung des Urheberrechts in der Informationsgesellschaft. Bundesvereinigung Deutscher Bibliotheksverbände e.V., Deutsche Gesellschaft für Informationswissenschaft und Informationspraxis e.V. Brief an Dr. Elmar Hucko vom Bundesministerium der Justiz. Berlin. Last visited: 18.12.2002. Available at:

http://www.urheberrecht.org/topic/Info-RiLi/st/schreiben_beger.pdf

Behlendorf (1999)

Behlendorf, Brian (1999): Open Source as a Business Strategy. In: DiBona, Chris/ Ockman, Sam/ Stone, Mark (eds.) (1999): *Open Sources — Voices From the Open Source Revolution*. Sebastopol. p. 149.

Beit-Arie (2001)

Beit-Arie, Oren et al. (September 2001): Linking to the Appropriate Copy: Report of a DOI-Based Prototype. In: *D-Lib Magazine*. Vol. 7. No. 9. Available at: <http://www.dlib.org/dlib/september01/caplan/09caplan.html>

Bell (1998)

Bell, Tom W. (1998): Fair use v. fared use: the impact of automated rights managements on copyright's fair use doctrine. In: 76 *N. Carolina L. Rev.* 557.

Bellare, et al. (1995)

Bellare, M./ Garay, J.A./ Hauser, R./ Herzberg, A./ Krawczyk, H./ Steiner, M./ Tsudik, G./ Waidner, M. (1995): iKP – A Family of Secure Electronic Payment Protocols. In: *First USENIX Workshop on Electronic Commerce*.

Bellare, et al. (2000)

Bellare, M./ Garay, J.A./ Hauser, R./ Herzberg, A./ Krawczyk, H./ Steiner, M./ Tsudik, G./ van Herreweghen, E./ Waidner, M. (2000): Design, implementation and deployment of the iKP secure electronic payment system. In: *IEEE Journal on Selected Areas in Communications*. 18(4). April 2000.

Benkler (1999)

Benkler, Yochai (1999): Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain. In: 74 *N.Y.U.L. Rev.* 354. 414. p. 421. Available at: <http://www.nyu.edu/pages/lawreview/74/2/benkler.pdf>.

Benkler (2000)

Benkler, Yochai (2000): An Unhurried View of Private Ordering Informations Transactions. In: *Vanderbilt Law Review* 53.

Benkler (2002)

Benkler, Yochai (2002): Intellectual Property and the Organization of Information Production. In: 22 *International Review of Law and Economics* 81.

Benjamin, Wigand (1995)

Benjamin, R.I./ Wigand, R.T. (1995): Electronic markets and virtual value chains on the Information Superhighway. In: *Sloan Management Review*. Winter. pp. 62–72.

Berman, Mathews (2003)

Berman, D.K./ Mathews, A.W. (2003): Is the record industry about to bust your teenager? In: *The Wall Street Journal*. January 28, 2003. pp. D1, D3.

Berrou, Glavieux, Titimajshima (1993)

Berrou, C./ Glavieux, A./ Titimajshima, P. (1993): Near Shannon limit error correctin coding: turbo codes. In: *Proceedings of the IEEE international conference on communication*. Geneva. pp. 1064–1070.

Berry (2002)

Berry, M. (2002): That's what I want — developing user-friendly DRM. Available at: <http://www.newarchitectmag.com/documents/s=2405/new1011653160573/index.html> Accessed: 16.05.2002.

Besen (1986)

Besen, Stanley M. (1986): Private Copying, Reproduction Costs, and the Supply of Intellectual Property. In: *Information Economics and Policy – Vol. 2*. pp. 5–22.

Besen, Kirby (1989)

Besen, Stanley M./ Kirby, Sheila N. (October 1989): Private Copying, Appropriability and Optimal Copying Royalties. In: *Journal of Law and Economics* – Vol. 32. pp. 255–280.

Bessen, Hunt (2003)

Bessen, James/ Hunt, Robert (2003): An empirical look at software patents. Available at: <http://www.idei.asso.fr/Commun/Conferences/Internet/Janvier2003/Papiers/Bessen.pdf>.

Bettis (1998)

Bettis, R. A. (1998): Commentary on “Redefining Industry Structure for the information Age” by J.L. Sampler. In: *Strategic Management Journal*. Vol. 19. pp. 357–361.

Beutelspacher (1996)

Beutelspacher, Albrecht (1996): *Kryptologie*. 5. Edition.

Bhatnagar, Misra, Raghav Rao (2000)

Bhatnagar, A./ Misra, S./ Raghav Rao, H. (2000): On Risk, Convenience, and Internet Shopping Behavior. In: *43 Communications of the ACM*. pp. 98–105.

Bibliotheksverband (2002)

Deutscher Bibliotheksverband (12.12.2002): Brief an die Mitglieder auf der Website des Deutschen Bibliotheksverbands. Last visited: 12.12.2002. Available at: <http://www.bibliotheksverband.de/dbv/rechtsgrundlagen/11112002urg.html>

BIC

EDItEUR and Book Industry Communication [BIC] (Nov 2000): “ONIX International Overview and Summary List of Data Elements”. Available at: <http://www.editeur.org/onixfiles1.2/ONIX%20Overview%20R1.2.PDF>.

Bide (1999)

Bide, M (January 1999): Directory of Persons: Outline Specification. EDItEUR ltd. Available at: <http://www.indecs.org/pdf/persons1.pdf>.

Bing (2001)

Bing, Friederike (2001): Die Verwertung von Urheberrechten. Eine ökonomische Analyse unter besonderer Berücksichtigung der Lizenzvergabe durch Verwertungsgesellschaften. Dissertation. Berlin.

Bishop (2003)

Bishop, Matt (2003): *Computer Security. Art and Science*. Boston, MA.

BITKOM (2000)

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (20.12.2000). Last visited: 20.12.2000. Available at: <http://www.bitkom.org/Presse/pr201200.htm>

BITKOM (2000a)

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (22.12.2000): Stellungnahme zum Zweiten Bericht der Bundesregierung über die urheberrechtliche Vergütung gemäß §§54ff UrhG (2. Vergütungsbericht). Berlin. Last visited: 22.12.2000. Available at: <http://www.bitkom.org>

BITKOM (2001)

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (21.3.2001): Beim Urheberrecht die Zeichen der digitalen Zeit erkennen. Hannover.

BITKOM (2001a)

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (23.3.2001a): Umfrage zu Urheberrechtsabgaben auf PCs, Drucker und ITK-Geräte: Verbraucher und Unternehmen lehnen Urheberrechtsabgaben ab. Berlin / Frankfurt/M.

BITKOM (2002)

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (2002): Urheberrechtliche Abgaben. Positionen und Fakten. Berlin.

BITKOM (2002a)

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (2002a): Wertschätzung und Wertschöpfung von Urheberrechten im digitalen Zeitalter. Zusammenfassung der Studie. Technische Schutzmaßnahmen in Verbindung mit Digital Rights Management Systemen — geeignete Systeme zur individuellen Lizenzierung. Im Auftrag der BITKOM Servicegesellschaft mbH durchgeführt von der TÜV Informationstechnik GmbH Essen. Berlin.

BITKOM (2002b)

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (3.2002): Stellungnahme. In: CDU/CSU-Bundestagsfraktion (2002): pp. 112–116.

BITKOM (2002c)

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (4.3.2002): BITKOM will zukunftsorientiertes Vergütungssystem für Urheber. Berlin. Last visited: 4.3.2002. Available at: <http://www.bitkom.org>.

BITKOM (2002d)

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (15.3.2002a): Digitale Kopierschutzlösungen und Digitales Rechtemangement. Digitale Rechteverwaltung (Digital Rights Management). Copyright Rightscom 2000.

BITKOM (2002e)

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (18.3.2002): BITKOM-Stellungnahme zum Referentenentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft. BITKOM nimmt Stellung zu dem Referentenentwurf aus dem Bundesjustizministerium vom 18.03.02. Berlin. Last visited: 18.3.2002. Available at: <http://www.bitkom.org>.

BITKOM (2002f)

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (23.3.2002): Stellungnahme zu den geplanten Erweiterungen der Vergütungspflicht nach §§54, 54a UrhG. Last visited: 23.2.2002. Available at: <http://www.bitkom.org/Politik/Stellungnahmen/st091000.html>

BITKOM (2002g)

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (30.7.2002): Stellungnahme zu §52 a Regierungsentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft. Berlin.

BITKOM (2002h)

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (1.8.2002): Urheberabgaben auf CD-Brenner. Pressemitteilung. Berlin. Last visited: 1.8.2002. Available at: <http://www.bitkom.org/>

BITKOM (2002i)

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (27.9.2002): BITKOM begrüßt Stellungnahme des Bundesrats zur Novellierung des Urheberrechtsgesetzes. Last visited: 27.9.2002. Available at: <http://www.bitkom.org>

BITKOM (2002j)

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (1.10.2002): Freiräume schaffen für Wachstum, Innovation und Arbeitsplätze. Ein 10-Punkte-Programm der ITK-Wirtschaft für die neue Legislaturperiode. Berlin. Last visited: 1.10.2002. Available at: [ttp://www.bitkom.org](http://www.bitkom.org).

BITKOM, BDI, VDZ, BDZV, VdS (2002)

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., Bundesverband der Deutschen Industrie, Verband Deutscher Zeitschriftenverleger, Bundesverband Deutscher Zeitungsverleger, VdS Bildungsmedien (16.12.2002). Last visited: 16.12.2002. Available at: http://www.urheberrecht.org/topic/Info-RiLi/st/Gemeins_Papier_2002-12-16.pdf

BITKOM, TÜViT (2001)

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., TÜViT (11.12.2001): Technische Schutzmaßnahmen in Verbindung mit Digital Rights Management Systemen — geeignete Systeme zur individuellen Lizenzierung. Berlin, Frankfurt/Main.

Bizer (2001)

Bizer, Johann (2001): Datenschutzgerechte Gestaltung des technischen Urheber-schutzes. In: 25 Datenschutz und Datensicherheit 12.

Black (2000)

Black, L. (2000): Understanding Consumer Demand to create business models that work. Webnoize Research. SGAE Conference. Madrid.

Blaze, Ioannidis, Keromytis (2001)

Blaze, M./ Ioannidis, J./ Keromytis, A.D. (2001): Offline micropayments without trusted hardware. In: Financial Cryptography – 5th International Conference (FC 2001), Proceedings.

Blocher (2001)

Blocher, Walter (2001) in: Walter, Michel M. (ed.)(2001): Europäisches Urheberrecht. Kommentar. Vienna.

Bloom, Griffith (2001)

Bloom, Nicholas/ Griffith, Rachel (2001): The Internationalisation of UK R&D. In: Fiscal Studies. 22. Jg. 3/2001. pp. 337–355.

Blum (1982)

Blum, M. (1982): Coin-flipping by telephone: A protocol for solving impossible problems. In: Proceedings of the 24th IEEE Computer Conference.

BMJ (2000)

Bundesministerium der Justiz (5.7.2000): Zweiter Bericht über die Entwicklung der urheberrechtlichen Vergütung gemäß §§54 ff. Urheberrechtsgesetz. (2. Vergütungsbericht). Last visited: 5. Juli 2000.

BMJ (2002)

Bundesministerium der Justiz (1.3.2002): Vorläufiges Ende der Mediation. Pressemitteilung. Pressemitteilung Nr. A7/02 Berlin, am 1. März 2002. Last visited: 1.3.2002. Available at: http://www.bmj.bund.de/frames/ger/themen/urheberrecht_und_patente/10000518

BMJ (2003)

Bundesministerium der Justiz (14.3.2003): Vorblatt. Antrag der Berichterstatter der Koalitionsfraktionen zum Entwurf eines Gesetzes zur Regelung des Urheberrechts in der Informationsgesellschaft. BT-Drs. 15/38. Stand/Abgerufen am: 14.3.2003. Online in: <http://www.urheberrecht.org/topic/Info-RiLi/ent/FormulBMJ-Vorblatt.pdf>

BMJ (2003a)

Bundesministerium der Justiz (14.3.2003): Zusammenstellung. Antrag der Berichterstatter der Koalitionsfraktionen zum Entwurf eines Gesetzes zur Regelung des Urheberrechts in der Informationsgesellschaft. BT-Drs. 15/38. mit den Beschlüssen des Rechtsausschusses. (6. Ausschuss). Stand/Abgerufen am: 14.3.2003. Online in: <http://www.urheberrecht.org/topic/Info-RiLi/ent/Antrag-Berichterst.pdf>

Bok (1982)

Bok, S. (1982): *Secrets: On the Ethics of Concealment and Revelation*. New York.

Boneh, Shaw (1998)

Boneh, D./ Shaw, J. (September 1998): Collusion-secure fingerprinting for digital data. *IEEE transactions on information theory*. Vol. 44. No. 5. pp. 1897–1905.

Boney, Tewfik, Hamdy (1996)

Boney, Laurence/ Tewfik, Ahmed H./ Hamdy, Khaled N. (17–23 June 1996): Digital watermarks for audio signals. *International Conference on Multimedia Computing and Systems*. Hiroshima, Japan. pp. 473–480.

Bonnert (2002)

Bonnert, Erich (2002): IDF: Mehr Details zu Intels Hardware-Verschlüsselung. In: *heise newsticker* (13 September 2002). Available at: <http://www.heise.de/bin/nt.print/newsticker/data/ciw-13.09.02-001/>. Last visited: 13.9.2002.

Borenstein, MacKieMason, Netz (2000)

Borenstein, Severin/ MacKieMason, Jeffrey K./ Netz, Janet S. (2000): Exercising Market Power in Proprietary Aftermarkets. 9 (2) *Journal of Economics & Management Strategy* 157.

Borges (1999)

Borges, Jorge Luis (1999): *John Wilkins' Analytical Language* (1942). translated in Weinberger, E. (ed.)(1999): *Borges: Selected Non-fictions*. Viking. New York.

Bornkamm (2002)

Bornkamm, Joachim (2002): Der Dreistufentest als urheberrechtliche Schrankenbestimmung — Karriere eines Begriffs. In: Ahrens et.al. (2002): p. 29.

Borland (2002)

Borland, J. (2002): ISPs gird for copyright fights. Available at: http://news.com.com/2100-1023-957023.html?tag=fd_ots. Accessed: 12.09.2002.

Börsenverein (2002)

Börsenverein des Deutschen Buchhandels (2002): Die Daten der Branche. 50 Jahre „Buch und Buchhandel in Zahlen“. Frankfurt/Main.

Börsenverein (2002a)

Börsenverein des Deutschen Buchhandels (3.2002): Stellungnahme. In: CDU/CSU-Bundestagsfraktion (2002): pp. 15–18.

Börsenverein, VdS (2002)

Börsenvereins des deutschen Buchhandels / VdS Bildungsmedien e.V. (21.8.2002): Gemeinsame Stellungnahme des Börsenvereins des deutschen Buchhandels und des VdS Bildungsmedien e.V. zum Regierungsentwurf (21. August 2002). Last visited: 21.8.2002. Available at: <http://www.urheberrecht.org/topic/Info-RiLi/st/ StellungnahmeBvRegE03.rtf>

Bortloff (1995)

Bortloff, Nils (1995): Der Tonträgerpiraterieschutz im Immaterialgüterrecht. Baden-Baden.

Bourret (2000)

Bourret, R. (March 2000): Namespace Myths Exploded. XML.com. Available at: <http://www.xml.com/pub/a/2000/03/08/namespaces/>.

Boyle (2000)

Boyle, James (2000): Cruel, Mean, or Lavish? Economic Analysis, Price Discrimination and Digital Intellectual Property. 53 Vanderbilt Law Review 2007.

Braun (2002)

Braun, Thorsten (3.2002): Beiträge im Wortprotokoll der Anhörung vom 16.11.2000. In: CDU/CSU-Bundestagsfraktion (2002): pp. 160, 166.

Brands (1993a)

Brands, S. (1993): An efficient off-line electronic cash system based on the representation problem. In: CWI Report. CS-R9323. Centrum voor Wiskunde en Informatica (CWI).

Brands (1993b)

Brands, S. (1993): Untraceable off-line cash in wallet with observers. In: Advances in Cryptology – CRYPTO '93 – 13th Annual International Cryptology Conference, Proceedings.

Brands (1995)

Brands, S. (1995): Off-line electronic cash based on secret-key certificates. In: Proceedings of the Second International Symposium of Latin American Theoretical Informatics (LATIN '95). April 1995.

Bremer (2002)

Bremer, Kathrin (3.2002): Beiträge im Wortprotokoll der Anhörung vom 16.11.2000. In: CDU/CSU-Bundestagsfraktion (2002): pp. 159, 163.

Brickell, Gemmell, Kravitz (1995)

Brickell, E./ Gemmell, P./ Kravitz, D. (1995): Trustee-based tracing extensions to anonymous cash and the making of anonymous change. In: Sixth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA'95). Proceedings.

Brynjolfsson, Kemerer (1995)

Brynjolfsson, E./ Kemerer, C. F. (1995): Network Externalities in Microcomputer Software: An Econometric Analysis of the Spreadsheet Market. In: Management Science. 42. pp. 1627–1647.

Buhse (2001)

Buhse, Willms (2001): Digital Rights Management for Music Filesharing Communities. Available at: http://e-business.fhbb.ch/eb/publications_nsf/id/94. Accessed: 17.8.2002.

Buhse (2002)

Buhse, Willms (2002): The Role of Digital Rights Management as a Solution for Market Uncertainties for Mobile Music. In: The International Journal on Media Management. Vol. 4. No. 3. Available at: <http://www.mediajournal.org/modules/pub/view.php/mediajournal-91>. Accessed: 4.11.2003.

Buhse (2003)

Buhse, Willms (2003): Wettbewerbsstrategien im Umfeld von Darknet und Digital Rights Management — Szenarien und Erlösmodelle für Onlinemusik. Dissertation. München (in print).

Bulletin (2002)

The Bulletin (20.11.2002): Seybold News & Views on Electronic Publishing. Vol. 8. No. 8.

Bundesrat (2002)

Deutscher Bundesrat (23.5.2002): Vermittlungsausschuss zum Urheberrecht angerufen. Available at: http://www.bundesrat.de/pr/pr79_03.html Last visited: 11.6.2003.

Bundesrat (2002a)

Deutscher Bundesrat – Wirtschaftsausschuss (12.9.2002): Entwurf eines Gesetzes zur Regelung des Urheberrechts in der Informationsgesellschaft. Ausschussempfehlung. Drucksache 684/02. Unveröffentlichtes anonymisiertes Protokoll.

Bundesrat (2002b)

Deutscher Bundesrat (27.9.2002): Entwurf eines Gesetzes zur Regelung des Urheberrechts in der Informationsgesellschaft. Drucksache 684/02 (Beschluss) Erster Durchgang. Available at: http://www.urheberrecht.org/topic/Info-RiLi/ent/stellungnahme_br.rtf

Bundestag (1997)

Deutscher Bundestag (1997): Enquete-Kommission „Zukunft der Medien in Wirtschaft und Gesellschaft — Deutschlands Weg in die Informationsgesellschaft“/ Deutscher Bundestag (1997): Neue Medien und Urheberrecht. Bundestagsdrucksache 13/8110. Bonn.

Bundestag (1998)

Deutscher Bundestag (1998): Enquete-Kommission „Zukunft der Medien in Wirtschaft und Gesellschaft — Deutschlands Weg in die Informationsgesellschaft“/ Deutscher Bundestag (1998): Deutschlands Weg in die Informationsgesellschaft. Bonn.

Bundestag (2001)

Deutscher Bundestag (14.3.2001): Antrag: Die Zukunft gehört der Individuallizenz – Vergütungsregeln für private Vervielfältigung im digitalen Umfeld. Drucksache 14/5577. Berlin.

Bundestag (2001a)

Deutscher Bundestag (27.9.2001): Antwort der Bundesregierung auf die Große Anfrage der Abgeordneten Steffen Kampeter, Dr. Norbert Lammert, Bernd Neumann (Bremen), weiterer Abgeordneter und der Fraktion der CDU/CSU. Drucksache 14/4290. 14. Wahlperiode 27.09.2001. Drucksache 14/6993. Berlin.

Bundestag (2002)

Deutscher Bundestag (14.11.2002): Plenarprotokoll der Bundestagssitzung v. 14.11.2002 (Auszug). Last visited: 13.12.2002. Available at: <http://www.bundestag.de/pp/10/150010j.zip>

Bundestag (2003)

Deutscher Bundestag (27.5.2003): Unterrichtung durch den Bundesrat. Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft. Drucksachen 15/38, 15/837. Anrufung des Vermittlungsausschusses. Drucksache 15/1066. Available at: <http://dip.bundestag.de/btd/15/010/1501066.pdf>. Last visited: 11.6.2003.

Bundestag — Rechtsausschuss (2003)

Deutscher Bundestag — Rechtsausschuss (9.4.2003): Union stimmt „schweren Herzens“ der Neuregelung des Urheberrechts zu Datenbanken. In: hib — heute im bundestag. Nr. 79. Stand/Abgerufen am 9.4.2003. Online in: <http://www.bundestag.de/aktuell/hib/2003.079/03.html>

Burk (2003)

Burk, Dan L. (forthcoming 2003): Anti-Circumvention Misuse, 48 UCLA Law Review. Draft available at <http://paper.ssrn.com/abstract=320961> (2002).

Burk, Cohen (2000)

Burk, Dan L./ Cohen, Julie E. (2000): FAIR USE INFRASTRUCTURE FOR COPYRIGHT MANAGEMENT SYSTEMS. Draft 8.18.00. Last visited: 12.6.2002. Available at: <http://www.cfp2002.org/program/fairuse.shtml>
Burk_cohen_2000.doc

Burk, Cohen (2001)

Burk, Dan L./ Cohen, Julie E. (2001): Fair Use Infrastructure for Rights Management Systems, 15 Harvard Journal of Law & Technology 41.

Burke (1996)

Burke, A.E. (1996): How Effective Are International Copyright Conventions in the Music Industry? In: Journal of Cultural Economics. Vol. 20. No. 1. pp. 51–66.

Burkert (1997)

Burkert, H. (1997): Privacy-Enhancing Technologies: Typology, Critique, Vision. In: Agre, P.E./ Rotenberg, M. (ed.)(1997): Technology and Privacy: The New Landscape. Cambridge, Massachusetts, London. pp. 125–142.

Burstein (1998)

Burstein, J. (1998): An implementation of MicroMint. Master's thesis. MIT.

bvkamera (2002)

Bundesverband Kamera (17.4.2002): Stellungnahme des Bundesverband Kamera zum Referentenentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft. München.

BVV (2002)

Bundesverband Audiovisuelle Medien (9.10.2002): Stellungnahme zu §52 a RegE. Last visited: 18.12.2002. Available at: http://www.urheberrecht.org/topic/Info-RiLi/st/BVV_Stellungn_52a.pdf

Bygrave (1998)

Bygrave, L.A. (1998): Data Protection Pursuant to the Right to Privacy in Human Rights Treaties. In: 6 International Journal of Law and Information Technology. pp. 247–284.

Bygrave (2001)

Bygrave, L.A. (2001): Electronic Agents and Privacy: A Cyberspace Odyssey 2001. In: 9 International Journal of Law and Information Technology. pp. 275–294.

Bygrave (2002a)

Bygrave, L.A. (2002): The Technologisation of Copyright: Implications for Privacy and Related Interests. In: 24 European Intellectual Property Review. pp. 51–57.

Bygrave (2002b)

Bygrave, L.A. (2002): Data Protection Law: Approaching its Rationale, Logic and Limits. Kluwer Law International. The Hague, London, New York.

Bygrave, Koelman (2000)

Bygrave, L.A./ Koelman, K.J. (2000): Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems. In: Hugenholtz (2000c): pp. 59–124.

— C —

Calabresi, Melamed (1972)

Calabresi, Guido & Melamed, A. Douglas (1972): Property Rules, Liability Rules, and Inalienability: One View of the Cathedral. 85 Harvarv Law Review 1089.

Camenisch, Maurer, Stadler (1996)

Camenisch, J./ Maurer, U./ Stadler, M. (1996): Digital payment systems with passive anonymity–revoking trustees. In: 1996 European Symposium on Research in Computer Security (ESORICS 96). Proceedings.

Camenisch, Maurer, Stadler (1997)

Camenisch, J./ Maurer, U./ Stadler, M. (1997): Digital payment systems with passive anonymity–revoking trustees. In: Journal of Computer Security. 5(1).

Camenisch, Piveteau, Stadler (1996)

Camenisch, J./ Piveteau, J.-M./ Stadler, M. (1996): An efficient fair payment system. In: 1st ACM Conference on Computer and Communications Security (CCS'96).

Caplan (1995)

Caplan, Priscilla (1995): You Call It Corn, We Call It Syntax-Independent Metadata for Document-Like Objects. In: The Public-Access Computer Systems Review 6. No. 4. pp. 19–23. Available at: <http://info.lib.uh.edu/pacsrev.html>

Caronni (1995)

Caronni, Germano (1995): Assuring ownership rights for digital images. In: Brüggermann, H.H./ Gerhardt-Häckl, W. (eds.)(1995): Proceedings of the conference on reliable IT systems (VIS'95). pp. 251–263.

Carpzov (1649)

Carpzov, Benedikt (1649): *Iurisprudentia ecclesiastica seu consistorialis*. Paris.

Cave (2002)

Cave, D. (2002): File sharing: Innocent until proven guilty. Available at: <http://www.buzzle.com/editorials/6-13-2002-20371.asp>. Accessed: 10.06.2002.

CDU/CSU-Bundestagsfraktion (3.2002)

Urheberrecht im digitalen Zeitalter. Eine Dokumentation zu Expertenhörungen in der CDU/CSU-Bundestagsfraktion. Berlin.

CEN/ISSS (2003)

CEN/ISSS (February 2003): Digital Rights Management Draft Report. Draft 1.1.

CEN/ISSS (2003a)

CEN/ISSS (February 2003): Digital Rights Management Draft Report. Draft 1.2. Available at: <http://www.cenorm.be/iss/iss/DRM/>.

CERT (2003)

CERT (January 2003): CERT/CC Statistics 1988–2002. Available at: http://www.cert.org/stats/cert_stats.html Last visitetd: 28 March 2003.

Chan, Frankel, Tsiounis (1998)

Chan, A./ Frankel, Y./ Tsiounis, Y. (1998): Easy come – easy go divisible cash. In: *Advances in Cryptology – EUROCRYPT '98 – International Conference on the Theory and Application of Cryptographic Techniques, Proceedings*.

Charron (2002)

Charron, C. (2002): What Content Will Consumers Pay For? In: *Forrester Research 2002*.

Chaum (1983)

Chaum, D. (1983): Blind signatures for untraceable payments. In: *Advances in Cryptology – CRYPTO '82. Proceedings*.

Chaum (1984)

Chaum, D. (1984): Blind signature systems. In: *Advances in Cryptology – CRYPTO '83. Proceedings*.

Chaum (1985)

Chaum, D. (1985): Security without identification: transaction systems to make big brother obsolete. In: *Communications of the ACM*. 28(10). October 1985.

Chaum (1986)

Chaum, D. (1986): Showing credentials without identification — signatures transferred between unconditionally unlinkable pseudonyms. In: *Advances in Cryptology – EUROCRYPT '85 – International Conference on the Theory and Application of Cryptographic Techniques. Proceedings*.

Chaum (1989)

Chaum, D. (1989): Privacy protected payments: Unconditional payer and/or payee untraceability. In: *Smart Card 2000. Proceedings*. North Holland.

Chaum, Fiat, Naor (1990)

Chaum, D./ Fiat, A./ Naor, N. (1990): Untraceable electronic cash. In: *Advances in Cryptology – CRYPTO '88 – 8th Annual International Cryptology Conference, Proceedings*.

Chaum, Pedersen (1993a)

Chaum, D./ Pedersen, T.P. (1993a): Transferred cash grows in size. In: *Advances in Cryptology – EUROCRYPT '92 – International Conference on the Theory and Application of Cryptographic Techniques. Proceedings*.

Chaum, Pedersen (1993b)

Chaum, D./ Pedersen, T.P. (1993b): Wallet databases with observers. In: *Advances in Cryptology – CRYPTO '92 – 12th Annual International Cryptology Conference. Proceedings.*

Chen (1998)

Chen, P.-Y. (1998): Pricing Strategies for digital information goods and online services on the Internet. Available at: <http://www.mba.ntu.edu.tw/~jtchiang/StrategyEC/eec/report1/report1.htm> Accessed: 10.06.2002.

Chen, Hott (2002)

Chen, P.-Y./ Hott, L. M. (2002): Measuring Switching Costs and the Determinants of Customer Retention in Internet-Enabled Businesses: A Study of the Online Brokerage Industry, *Information Systems Research*. 13. 3. pp. 255–274.

Chen, Wornell (2001)

Chen, B./ Wornell, G.W. (May 2001): Quantisation index modulation: a class of provably good methods for digital watermarking and information embedding. In: *IEEE transaction on information theory*. Vol. 47. No. 4. pp. 1423–1443.

Cheng, Sims, Teegen (1997)

Cheng, H.K./ Sims, R./ Teegen, H. (1997): To Purchase or to Pirate Software: An Empirical Study. In: *Journal of Management Information Systems* (1997) 13. pp. 49–60.

Chiappetta (2000)

Chiappetta, Vincent (2000): The Desirability of Agreeing to Disagree: The WTO, TRIPS, International IPR Exhaustion and a Few Other Things. 21 *Michigan Journal of International Law* 333.

Chicola, Farber, Karatsu, Liu, Richter (1998)

Chicola, Jason/ Farber, Dawn/ Karatsu, Mami/ Liu, Joseph/ Richter, Karl/ Tilly, John (1998): Digital Rights Architectures for Intellectual Property Protection — Legal/Technical Architectures of Cyberspace. Available at: <http://www.swiss.ai.mit.edu/6805/student-papers/fall98-papers/trusted-systems/trustsys.html>

Christianson, Crispo, Lomas, Roe (1998)

Christianson, Bruce/ Crispo, Bruno/ Lomas, Mark/ Roe, Michael (1998): *Security Protocols*. 5th International Workshop. Paris, France. April 1997. Proceedings. Berlin, Heidelberg, New York.

Ciborra (1993)

Ciborra, C.U. (1993): *Teams, markets and systems: Business innovation and information technology*. Cambridge, England.

Clark (2002)

Clark, Drew (17.4.2002): Intellectual Property: Panelists Ponder Middle Ground On Anti-Piracy Technology. In: *National Journal's Technology Daily*. Last visited: 17.4.2002. Available at: <http://nationaljournal.com/>

Clark (2003)

Clark, Kendall G. (2003): Creative Comments: On the Uses and Abuses of Markup. Last visited: 15.1.2003. Available at <http://www.xml.com/pub/a/2003/01/15/creative.html>.

Clarke

Clarke, R.: A defendant class action law suit. Available at: <http://www.kentlaw.edu/perritt/honorsrscolars/clarke.html>

Clarke (1996)

Clarke, R. (18th October 1996): Identification, Anonymity and Pseudonymity in Consumer Transactions: A Vital Systems Design and Public Policy Issue. Presentation to Conference on "Smart Cards: The Issues". Sydney. Available at: <http://www.anu.edu.au/people/Roger.Clarke/DV/AnonPsPol.html>

Clarke, Sandberg, Wiley, Hong (2000)

Clarke, I./ Sandberg, O./ Wiley, B./ Hong, T. (2000): Freenet: A distributed information storage and retrieval system. In: International Workshop on Design Issues in Anonymity and Unobservability.

Clement, Nerjes, Runte (2002)

Clement, M./ Nerjes, G./Runte, M. (2002): Content-Distribution im Zeitalter von Peer-to-Peer-Technologien. In: Schoder, D./ Fischbach, K./ Teichmann, R. (ed.)(2002): Peer-to-Peer (P2P): Ökonomische, technologische und juristische Perspektiven. Heidelberg. pp. 71–80.

Coase (1937)

Coase, Ronald H. (1937): The Nature of the Firm. In: *Economica*. 14(16). pp. 386–405.

Coase (1960)

Coase, Ronald H. (1960): The Problem of Social Cost. In: *Journal of Law and Economics*. 3. Jg. 1/1960. pp. 1–44.

Cohen (1996)

Cohen, Julie E. (1996): A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace. In: 28 *Connecticut Law Review* 981.

Cohen (1998)

Cohen, Julie E. (1998): Lochner in Cyberspace: The New Economic Orthodoxy of "Rights Management". In: 97 *Michigan Law Review* 462.

Cohen (2000)

Cohen, Julie E. (2000): Copyright and the Perfect Curve. In: 53 *Vanderbilt Law Review* 1799.

Cohen (2003)

Cohen, Julie E. (2003): DRM and Privacy. In: *Berkeley Technology Law Journal*. Vol. 18. Available at: <http://www.law.georgetown.edu/faculty/jec/drmandprivacy.pdf>. Last visited: 3.4.2003.

Cohen (2003a)

Cohen, Julie E. (2003): DRM and Privacy. In: *Communications of the ACM*. No. 4. Vol. 46. pp. 46–50.

Cohen, Levinthal (1990)

Cohen, Wesley M./ Levinthal, Daniel A. (1990): Absorptive capacity: a new perspective on learning and innovation. In: *Administrative Science Quarterly*. 35. Jg. 1/1990. pp. 128–153.

Cohen, Zemor (1994)

Cohen, G.D./ Zemor, G. (November 1994): Intersecting codes and independent families. *IEEE transactions on information theory*. Vol. 40. No. 6. pp. 1872–1881.

Collberg, Thomborson, Low (1997)

Collberg, C./ Thomborson, C./ Low, D. (July 1997): A Taxonomy of Obfuscating Transformations. Technical Report 148. Department of Computer Science. University of Auckland.

Collberg, Thomborson, Low (1998)

Collberg, C./ Thomborson, C./ Low, D. (May 1998): Breaking Abstractions and Unstructuring Data Structures. IEEE International Conference on Computer Languages. Chicago.

Collberg, Thomborson (2002)

Collberg, C./ Thomborson, C. (June 2002): Watermarking, Tamper-Proofing, and Obfuscation — Tools for Software Protection. IEEE Transactions on Software Engineering. Vol. 28. No. 6.

Committee of Commerce of the House of Representatives (July 22nd, 1998)

H.R. Rep. No. 105-551. Part 2. 105th Cong. 2d. Sess (July 22nd, 1998).

Committee on Intellectual Property Rights and the Emerging Information Infrastructure (2000)

Committee on Intellectual Property Rights and the Emerging Information Infrastructure (2000): The digital dilemma: intellectual property in the information age. National Research Council. Washington, D.C. Available at: http://www.nap.edu/html/digital_dilemma/.

Communication from the Commission: Follow-up to the Green Paper on Copyright and Related Rights in the Information Society. COM (96) 568 final. 20.11.1996.

Communication from the Commission to the Council, the European Parliament and the Economic and Social Committee: Follow-up to the Green Paper on combatting counterfeiting and piracy in the single market. COM (2000) 789 final. 30.11.2000.

ComputerWire Staff (2003)

ComputerWire Staff (2003): Trusted Computing Group Will Aid Microsoft's Palladium. In: Yahoo News (9 April 2003): Available at: <http://uk.news.yahoo.com/030409/221/dxc8s.html> Last visited: 12 April 2003.

Conner, Rumelt (1991)

Conner, Kathleen R./ Rumelt, Richard P. (1991): Software Piracy: an Analysis of Protection Strategies. In: Management Science. Vol. 37 (2). Februar 1991. pp. 125–139.

ContentGuard (2000)

ContentGuard, Inc. (2000): Extensible rights Markup Language (XrML) Specification Version 2.0. White Paper. Available at: <http://www.xrml.org/>.

Cooper, Frieze (2001)

Cooper, C./ Frieze, A. (2001): A general model of web graphs. In: Proceedings of the 9th Annual European Symposium on Algorithms. 500–511

CPSS BIS (1996)

Committee on Payment and Settlement Systems (CPSS), Bank for International Settlements (BIS): Security of electronic money. May 1996.

CPSS BIS (2000)

Committee on Payment and Settlement Systems (CPSS), Bank for International Settlements (BIS): Survey of electronic money developments. May 2000.

CPTWG

Available at: <http://www.cptwg.org>.

Coase (1937)

Coase, R. (1937): The Nature of the Firm. In: *Economica* (4). pp. 386–405.

- Copyright and Related Rights on the Threshold of the 21st Century. International Conference. Florence/Italy. June 2–4, 1996
- Council Decision of 16 March 2000 on the approval, on behalf of the European Community, of the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty (2000/278/EC). OJ L 89/6 of 11.4.2000.
- Council Directive of 14 May 1991 on the legal protection of computer programs (91/250/EEC). OJ L 122/42 of 17.5.91
- Council Directive 92/100/EEC of 19.11.1992 on rental right and lending right and on certain rights related to copyright in the field of intellectual property. OJ L 346/61 of 27.11.92
- Council Directive 93/83/EEC of 27.9.1993 on the co-ordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission. OJ L 248/15 of 6.10.93
- Council Directive 93/98/EEC of 29.10.1993 harmonising the term of protection of copyright and certain related rights. OJ L 290/9 of 24.11.93
- Cox, Killian, Leighton, Shamoon (1996)
Cox, Ingemar J./ Killian, J./ Leighton, T./ Shamoon, T. (June 1996): A secure robust watermark for multimedia. In: Proceedings of first international workshop on information hiding. Cambridge, England. pp. 183–206.
- Cox, Miller (1997)
Cox, Ingemar J./ Miller, Matt L. (10–13 February 1997): A review of watermarking and the importance of perceptual modelling. In: Rogowitz, Bernice E./ Pappas, Thrasyvoulos N. (ed.)(1997): Proceedings of the SPIE conference on human vision and electronic imaging II. San Jose, California, U.S.A. pp 92–99.
- Cranor (2002)
Cranor, Lorrie F. (2002): Web Privacy with P3P. Sebastopol.
- Craver et al. (2001)
Craver, S.A./ Wu, M./ Liu, B./ Stubblefield, A./ Swartzlander, B./ Wallach, D.S./ Dean, D./ Felton, E. (August, 2001): Reading between the lines: lessons from the SDMI challenge. In: Proceedings of the 10th USENIX Security Symposium. Washington, D.C.
- Creative Commons (2002)
Creative Commons (2002): Cultivating the Public Domain. White Paper. Available at: <http://www.creativecommons.org/>.
- Cremer et al. (2001)
Cremer, M./ Froba, B./ Hellmuth, O./ Herre, J./ Allamanche, E. (2001): AudioID: Towards Content-Based Identification of Audio Material. In: Proc. 110th Audio Engineering Society Convention. Amsterdam, NL.
- Creativity & Intellectual Property Rights: Evolving Scenarios and Perspectives. International Conference. Vienna/Austria. July 12–14, 1998.
- Crosby et al. (2001)
Crosby, Scott/ Goldberg, Ian/ Johnson, Robert/ Song, Dawn/ Wagner, David (2001): A Cryptanalysis of the High-Bandwidth Digital Content Protection System. In: Sander (2001): p. 192.

Cross Industry Working Team (1997)

Cross Industry Working Team [XIWT] (1997): Managing Access to Digital Information: An Approach based on Digital Objects and Stated Operations. Available at: <http://www.xiwt.org/documents/ManagAccess.html>

Crowston, Wigand (1999)

Crowston, K./ Wigand, R.T. (1999): Real-estate war in cyberspace: An emerging electronic market? In: *Electronic Markets*. 9(1/2). pp. 1–8.

Cryptography (2002)

Cryptography Mailing List. Available at: <http://www.mail-archive.com/cryptography%40wasabisystems.com/>. Last visited: 30 March 2003.

Cypherpunks (2002)

Cypherpunks Mailing List. Available at: <http://www.inet-one.com/cypherpunks/>. Last visited: 30 March 2003.

— D —

Dabek, Brunskill, Kaashoek, Karger, Morris, Stoica, Balakrishnan (2001)

Dabek, F./ Brunskill, E./ Kaashoek, M.F./ Karger, D./ Morris, R./ Stoica, I./ Balakrishnan, H. (2001): Building peer-to-peer systems with Chord, a distributed lookup service. In: *Proceedings of the Eighth IEEE Workshop on Hot Topics in Operating Systems (HotOS-VIII)*. pp. 81–86

Dankwardt (2002)

Dankwardt, Kevin (2002): Are Non-GPL Loadable Linux Drivers Really Not a Problem? Available at <http://www.linuxdevices.com/articles/AT5041108431.html> (last modified Sept. 30, 2002).

Datenschutzbeauftragte des Bundes und der Länder (2003)

TCPA darf nicht zur Aushebelung des Datenschutzes missbraucht werden. Entschließung der 65. Konferenz der Datenschutzbeauftragten am 27./28. März 2003 in Dresden. Available at <http://www.datenschutz.mvnet.de/beschlue/ent65.html> (March 27/28, 2003).

Däubler-Gmelin (1999a)

Däubler-Gmelin, Herta (1999a): Private Vervielfältigung unter dem Vorzeichen digitaler Technik. überarbeitete Fassung der am 20.8.1999 auf der POPKOMM in Köln gehaltenen Rede. Last visited: 20.1.2000. Available at: http://www.bmj.bund.de/misc/reden/r_992008.htm

David (2000)

David, Paul A. (2000): A tragedy of the public knowledge “commons”? All Souls College. Oxford & Stanford University. WP04/00, available at: <http://www.oiprc.ox.ac.uk/ejwp0400.html>

Davida, Frankel, Tsiounis, Yung (1997)

Davida, G./ Frankel, Y./ Tsiounis, Y./ Yung, M. (1997): Anonymity control in e-cash systems. In: *Financial Cryptography, First International Conference 1997 (FC'97)*. Proceedings.

Davies (1996)

Davies, G. (1996): A history of money from ancient times to the present day. University of Wales.

DBV (1999)

Deutscher Bibliotheksverband e.V. (3.12.1999): Brief an die deutschen Mitglieder des Europäischen Parlamentes. Geänderter Vorschlag für eine Richtlinie zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft. KOM (1999)...endg. 97/0359/COD -und Konsolidierte Fassung des Artikels 5 (Dok.-Nr. 9734/99, vom 30. Juni 1999). Berlin. Last visited: 24.11.2002. Available at: <http://www.bibliotheksverband.de/dbv/dokumente/2-12-99Begleit.doc>

DBV (1999a)

Deutscher Bibliotheksverband e.V. (3.12.1999a): Stellungnahme und Formulierungsvorschläge zu Artikel 5 des Geänderten Richtlinienvorschlags. Berlin. Available at: <http://www.bibliotheksverband.de/dbv/dokumente/2-12-99Stellungnahme.doc>

DBV (2001)

Deutscher Bibliotheksverband e.V. (25.7.2001): Stellungnahme des Deutschen Bibliotheksverbands e.V. zur Umsetzung der EU-Richtlinie zur Harmonisierung des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft in das deutsche Urheberrechtsgesetz. Rechtskommission des EDBI im Auftrag des Deutschen Bibliotheksverbandes e.V. Berlin. Available at: <http://www.bibliotheksverband.de/dbv/rechtsgrundlagen/DBV-BMJ-Stellungnahme-25-7-2001.doc>

Dean (2002)

Dean, Drew (30.1.2002): Anti-circumvention regulation and cryptography research. Vortrag am 30.1.2002 auf der II. Digital Rights Management Konferenz am 29. und 30.1.2002 des Forschungsverbunds Datensicherheit im Haus der Wirtschaft. Berlin. Last visited: 30.1.2002. Available at: http://www.eurubits.de/drm/drm_2002/audio/dean.mp3

Decision on submission for preliminary ruling of LG Frankfurt/M of 12.7.2001 (Case C-418/01, IMS Health GmbH & Co. OHG vs. NDC Health GmbH & Co. KG). OJ C 3/16 of 5.1.2002.

Decision of the European Commission of 3.7.2001 (COMP D3/38.044 – NDC Health./.IMS Health). OJ L 59/18 of 28.2.2002.

Decision of the ECJ of first Instance of 26.10.2001 (Case T-184/01 R, IMS Health vs. Commission of the European Communities). OJ C 144/45 of 15.6.2002.

DeMartini, Wang, Wragg (2002)

DeMartini, T./ Wang, X./ Wragg, B. (July 2002): MPEG 21 Part 5: Rights Expression Language. Moving Pictures Expert Group (MPEG). ISO/IEC JTC 1/SC 29/WG 11/N494.

Depoorter, Parisi (2002)

Depoorter, B./ Parisi, F. (2002): Fair Use and Copyright Protection: a price theory explanation. In: International Review of Law and Economics – 21. pp. 453–473.

Dessemontet (1974)

Dessemontet, Francois (1974): le Savoir-Faire industriel. Definition et protection du “know-how” en droit américain. Genf.

Detecon (2002)

Detecon (2002): p2p – Die Hoffnung stirbt zuletzt. White Paper.

Deutsche Bank (2000)

Deutsche Bank (2000): New Media Mechanics — Value of Content Online.

Devanbu, Stubblebine (2000)

Devanbu, P./ Stubblebine, S. (2000): Software Engineering for Security: a Roadmap. ICSE 2000 Special Vol. on the Future of Software Engineering.

Devaraj, Fan, Kohli (2002)

Devaraj, S./ Fan, M./ Kohli, R. (2002): Antecedents of B2C Channel Satisfaction and Preference: Validating e-Commerce Metrics. *Information Systems Research*. 13. 3. pp. 316–333.

v. Diemar (2002)

v. Diemar, U. (July 2002): Kein Recht auf Privatkopien — Zur Rechtsnatur der gesetzlichen Lizenz zu Gunsten der Privatvervielfältigung. In: GRUR 2002. pp. 587–593.

Dierks, Allen (1999)

Dierks, C./ Allen, C. (1999): The TLS protocol version 1.0. RFC 2246. January 1999.

Dietz (1985)

Dietz, Adolf (1985): Die Entwicklung des Urheberrechts der Bundesrepublik Deutschland von 1979 bis Anfang 1984. In: UFITA. Vol. 100. p. 15.

Dietz (1988)

Dietz, Adolf (1988): Urheberrecht im Wandel. Paradigmenwechsel im Urheberrecht? In: Dittrich (1988): Woher kommt das Urheberrecht und wohin geht es? Vienna. p. 200.

Diffie, Hellman (1976)

Diffie, W. / Hellman, M.E. (Nov. 1976): New Directions in Cryptography. In: IEEE Transactions on Information Theory. pp. 644–654.

DIHK (2002)

Deutscher Industrie- und Handelstag (heute: Deutsche Industrie- und Handelskammertag)(3.2002): Stellungnahme. In: CDU/CSU-Bundestagsfraktion (2002): pp. 116–117.

DIHK (2002)

Deutscher Industrie- und Handelskammertag (2.5.2002): Stellungnahme des Deutschen Industrie- und Handelskammertages zum Referentenentwurf. Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft. Berlin.

Directive 1996/9/EC

Directive 1996/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases. OJ L 77/20 of 27.3.96.

Directive 1998/34/EC

Directive 1998/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on information society services, OJ L 298, 17. 10. 1989. Directive as amended by Directive 97/36/EC of the European Parliament and of the Council (OJ L 202, 30. 7. 1997, p. 60).

Directive (1999)

Directive of the European Parliament and of the Council on a Community Framework for Electronic Signatures. Official Journal of the European Communities. 13 December 1999.

Directive 2001/19/EG

Directive 2001/19/EG of the European Parliament and the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society, OJ L 167 of 22.06.2001, p. 10 ff.
http://europa.eu.int/eur-lex/de/dat/2001/1_167/1_16720010622de00100019.pdf

Directive 2001/29/EC

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. Official Journal L167,22/06/2001 P. 0010-0019. The directive can be found at <http://europa.eu.int/eur-lex/>.

Directive 2000/31/EC

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on electronic commerce). OJ L 178/1 of 17.7.2000.

Directive 2001/84/EC

Directive 2001/84/EC of the European Parliament and of the Council of 27 September 2001 on the resale right for the benefit of the author of an original work of art. OJ L 272/32 of 13.10.2001

Directorate-General

Information Society Directorate-General of the European Commission DRM Working Group Presentations and Minutes. Available at: http://europa.eu.int/information_society/topics/multi/digital_rights/events/index_en.html

Dix (2002)

Dix, Alexander (30.1.2002): Digitales Urheberrechts-Management (DRM) und Datenschutz Statement bei der Konferenz „II. Digital Rights Management 2002“ am 30. Januar 2002 in Berlin. Berlin.

Dixon, Greenhalgh (2002)

Dixon, Pdraig/ Greenhalgh, Christine (2002): The economics of intellectual property: a review to identify themes for future research. Available at: <http://www.oiprc.ox.ac.uk/EJWP0502.html> EJWP 05/02/2002.

DJV (2002)

Deutscher Journalistenverband (9.4.2002): Stellungnahme des Deutschen Journalistenverbandes e.V. zum Referentenentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft. Bonn.

DMMV (2001)

Deutscher Multimedia Verband (13.11.2001): Stellungnahme des Deutschen Multimedia Verbandes zur Umsetzung der EU-Urheberrechtsrichtlinie 2001/29/EG zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft in deutsches Recht. Berlin / München.

DMMV (2002)

Deutscher Multimedia Verband (18.4.2002): Stellungnahme des Deutschen Multimedia Verbandes zum Referentenentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft. Berlin, München.

DMMV (2002a)

Deutscher Multimedia Verband (9.9.2002): Stellungnahme des Deutschen Multimedia Verbandes zum Regierungsentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft. Last visited: 12.12.2002. Available at: http://www.dmmv.de/de/data/doc/2501_006_035_stellgn_reg_entwurf_020909.doc

DMMV, VPRT (2002)

Deutscher Multimedia Verband, Verband Privater Rundfunk & Telekommunikation (9.2002): Erste Schlussfolgerungen der Verbände auf Grundlage der Ergebnisse der Gutachten zu den „Anforderungen an die gesetzliche Regulierung zum Schutz digitaler Inhalte unter Berücksichtigung der Effektivität technischer Schutzmechanismen“. Last visited: 30.9.2002. Available at: <http://www.dmmv.de/shared/data/zip/forderungskatalog.zip>

DMMV, VPRT (2002a)

Deutscher Multimedia Verband, Verband Privater Rundfunk & Telekommunikation (12.9.2002): Medienverbände fordern effektiven Schutz digitaler Inhalte Gemeinsame Gutachten belegen Handlungsbedarf in Sachen Piraterie. Last visited: 12.9.2002. Available at: http://www.dmmv.de/shared/data/doc/2300_001_vpvt.dmmv_datenpiraterie_020911.doc

Dugelay, Roche (1999)

Dugelay, Jean-Luc/ Roche, S. (1999): Fractal transform based large digital watermark embedding and robust full blind extraction. In: Proceedings of IEEE International Conference on Multimedia Computing and Systems. ICMCS 1999. 7–11 June, 1999. Florence, Italy. Proceedings. Vol. II. pp. 1003–1004.

Doglio, Richeri (1996)

Doglio, D./ Richeri, G. (1996): The Economics of Publishing: Prospects for Online Distribution. Centro Studi Salvador. Telecom Italia. Venice.

Doherty (2002)

Doherty, Sean (2002): Managing your digital rights. In: Network Computing. 15.09./2002. pp. 65–68.

Dölemeyer, Klippel (1991)

Dölemeyer, Barbara/ Klippel, Diethelm (1991). In: Beier et.al. (ed.)(1991): Festschrift 100 Jahre GRUR (Vol. 1). Weinheim.

DOI (2003)

International DOI Foundation (2003): DOI Handbook Version 2.6.0. Available at: <http://www.doi.org/hb.html>.

DOI Standard

The Digital Object Identification standard, homepage at www.doi.org.

DOI News (2001)

International DOI Foundation (Oct 2001): DOI News. Available at: <http://www.doi.org/news/010925-indecs2.html>

Dölemeyer, Klippel (1991)

Dölemeyer, Klippel (1991): Der Betrag der deutschen Rechtswissenschaft zu Theorie des gewerblichen Rechtsschutzes und Urheberrechts. In: Gewerblicher Rechtsschutz und Urheberrecht in Deutschland. Festschrift zum 100jährigen Bestehen der Deutschen Vereinigung für gewerblichen Rechtsschutz und Urheberrecht und ihrer Zeitschrift. Weinheim. Vol. 1.

- Dördermann (1999)
 Dördermann, Jörg-Eckhard (1999): Gedanken zur Zukunft der Staatsaufsicht über Verwertungsgesellschaften. In: GRUR 1999. Heft 10. pp. 890–896.
- Downes, Mui, (1998)
 Downes, L./ Mui, Ch. (1998): Unleashing the Killer App. Digital Strategies for Market Dominance. Harvard. M.A.
- Dreier (1993)
 Dreier, Thomas (1993): Copyright Digitized: Philosophical Impacts and Practical Implications for Information Exchange in Digital Networks. In: WIPO Worldwide Symposium on the Future of Copyright and Neighboring Rights. March 1993.
- Dreier (1997)
 Dreier, Thomas (1997). In: Schricke (1997).
- Dreier (2001)
 Dreier, Thomas (2001): Primär- und Folgemärkte. In: Schricke, Dreier, Kur (2001). p. 51.
- Dreier (2002a)
 Dreier, Thomas (2002): Die Umsetzung der Urheberrechtsrichtlinie 2001/29/EG in deutsches Recht. In: ZUM 2002.
- Dreier (2002b)
 Dreier, Thomas (2002): Konvergenz und das Unbehagen des Urheberrechts. In: Ahrens et.al. (2002): p. 73.
- Dreier, Senftleben (2001)
 Dreier, Thomas/ Senftleben, Martin (2001): Das Verhältnis des Urheberrechts zum Vertragsrecht — Grenzen des Vertragsrechts durch Intellectual Property Law. In: Lejeune, Mathias (ed.)(2001): Der E-Commerce-Vertrag nach amerikanischem Recht. Cologne. p. 81.
- Druck Gegen Abgaben (2001)
 Initiative Druck Gegen Abgaben (11.10.2001): Digitales Rechtemanagement sichert die Zukunft des Internet. Pressemitteilung. Last visited: 11.10.2001. Available at: http://www.druck-gegen-abgaben.de/pressroom/news_02.html
- Druck Gegen Abgaben (2001a)
 Initiative Druck Gegen Abgaben (11.10.2001b): Die pauschale Urheberrechtsabgabe eine „Sondersteuer“ auf PC-Drucker? Last visited: 11.10.2001b. Available at: http://www.druck-gegen-abgaben.de/pressroom/news_01.html
- Druck Gegen Abgaben (2001b)
 Initiative Druck Gegen Abgaben (18.10.2001): Sondersteuer für Drucker gefährdet die deutsche Druckerindustrie. Pressemitteilung. Last visited: 18.10.2001. Available at: http://www.druck-gegen-abgaben.de/pressroom/news_03.html
- Druck Gegen Abgaben (2001c)
 Initiative Druck Gegen Abgaben (11.2001): Stellungnahme der Drucker-Unternehmen zur Umsetzung der EU-Richtlinie zum Urheberrecht. Last visited: 1.12. 2001. Available at: http://www.druck-gegen-abgaben.de/pressroom/news_06.html

Druck Gegen Abgaben (2001d)

Initiative Druck Gegen Abgaben (9.11.2001): Hewlett-Packard kritisiert Forderungen von GEMA-Chef Kreile zu Urheberrechtsabgaben auf PCs und Drucker. Pressemitteilung. Last visited: 9.11.2001. Available at: http://www.druck-gegen-abgaben.de/pressroom/news_05.html

Druck Gegen Abgaben (2002)

Initiative Druck Gegen Abgaben (30.4.2002): Pauschale Urheberrechtsabgaben vernichten Arbeitsplätze. München. Last visited: 30.4.2002. Available at: http://www.druck-gegen-abgaben.de/pressroom/news_09.html

Druck Gegen Abgaben (2002a)

Initiative Druck Gegen Abgaben (31.7.2002): Kabinett befürwortet Sondersteuer auf digitale IT-Geräte Druckerhersteller enttäuscht über mangelnde Zukunftsorientierung der Bundesregierung. Last visited: 31.7.2002. Available at: <http://www.druck-gegen-abgaben.de>

Druey (1995)

Druey, Jeen Nioclas (1997): Information als Gegenstand des Rechts. Zürich.

DublinCore

The Dublin Core Metadata Initiative, homepage at: <http://dublincore.org/>.

Duhl, Kevorkian (2001)

Duhl, Joshua / Kevorkian, Susan (October 2001): Understanding DRM Systems — An IDC Technical White Paper. Available at: <http://www.intertrust.com/main/research/whitepapers/IDCUnderstandingDRMSystemms.pdf>. Last visited: 21 February 2003.

Dünnwald (1997)

Dünnwald, Rolf (1997): GVL. In: Moser, Scheumann (1997): pp. 680–684.

Durlacher (2001)

Durlacher (2001): Impacts of Digital Distribution on the Music Industry. Research Report.

Dusch, Sprenger (2003)

Dusch, Christiane/ Sprenger, Bettina (2003): Rechtemanagement in Multimediaprojekten an Hochschulen. In: DUZ extra Nr. 1–2. p. I

Dusollier (1999)

Dusollier, Séverine (1999): Electrifying the Fence: The legal protection of technological measures for protecting copyright. E.I.P.R. 1999. No. 21/6 pp. 285–297.

Dusollier (2000)

Dusollier, Séverine (2000): Incidences et réalités d'un droit de contrôler l'accès aux œuvres en droit européen. In Copyright: A right to control access to works? Cahier du CRID No. 18. Bruylant. Brussels.

DWS (2003)

Digital World Services, LLC. (January 2003): The ADo²RA System. Technical White Paper. Available at: <http://www.dwsco.com/adora/>.

Dykstra (2002)

Dykstra, Gail (2002): Where is DRM headed now? In: Information Today. November/2002. pp. 29–30, 49.

— E —

- Ears & Eyes (2001)
Ears & Eyes (2001): Bezahlter Content im Internet — Grundlagestudie zu den Einstellungen der User.
- Eastlake, Boesch, Crocker, Yesil (1996)
Eastlake, D./ Boesch, B./ Crocker, S./ Yesil, M. (1996): CyberCash Credit Card Protocol Version 0.8. In: RFC 1898. February 1996.
- ECJ of 17.5.1988 (“Warner Bros. ./ Christiansen”). Case 158/86. ECJ Reports 1988 p. 02605.
- ECJ of 24.1.1989 (“EMI Electrola ./ Patricia”), Case 341/87. ECJ Reports 1989 p. 00079
- EDB (1998)
Ehemaliges Deutsches Bibliotheksinstitut (7.9.1998): Elektronische Information und Urheberrecht. Gemeinsames Statement BDB, DBI. BIBLIOTHEKS-DIENST. Heft 9.
- Edgeworth (1881)
Edgeworth, F.Y. (1881): *Mathematical Psychics: An Essay on the Application of Mathematics to the Moral Sciences*. London.
- EDItEUR
EDItEUR: ONIX Product Information Standards. Available at <http://www.editeur.org/>.
- Ehlers (1994)
Ehlers, Hans-Jürgen (1994): Identification Numbering in the Book, Library and Information World. In: *ISBN Review* – 15. pp. 89–214.
- Einhorn (2002)
Einhorn, Michael A. (2002): Digital Rights Management and Access Protection: An Economic Analysis. In: *Proceedings of the ALAI Congress, June 13–17, 2001*. New York. Available at: http://www.law.columbia.edu/conferences/2001/1_program_en.htm
- Eisenberg (2001)
Eisenberg, Rebecca S. (2001): Bargaining Over the Transfer of Proprietary Research Tools: Is This Market Failing or Emerging? In: Dreyfuss, Rochelle C./ Zimmermann, Diane L./ First, Harry (ed.) (2001): *Expanding the Boundaries of Intellectual Property: Innovation Policy for the Knowledge Society*. Oxford. p. 223.
- Elaborate Bytes AG (2002)
CloneCD 4. Elaborate Bytes AG. Cham, Switzerland. Last visited: 8.12.2002. Available at: http://elby.ch/english/products/clone_cd/index.html
- Electronic Frontier Foundation (2003): Unintended Consequences: Four Years under the DMCA. Available at http://www.eff.org/IP/DRM/DMCA/20030103_dmca_consequences.pdf (Jan. 9, 2003).
- Elkin-Koren (1998)
Elkin-Koren, Niva (1998): Copyrights in Cyberspace — Rights Without Laws? In: *73 Chicago-Kent Law Review* (1998). p. 1155.
- Elkin-Koren, Netanel (2002)
Elkin-Koren, Niva/ Netanel, Neil W. (ed.) (2002): *The Commodification of Information*. The Hague.

Elkin–Koren, Salzberger (1999)

Elkin-Koren, Niva/ Salzberger, Eli M. (1999): Law and Economics in Cyberspace. In: *International Review of Law and Economics* 19.

Emch (2002)

Emch, Eric R. (March 2002): Does Opportunism Explain Markups in Laser Printer Toner and Memory? No and Yes. Evidence on Pricing in Laser Printer Aftermarkets. Available at <http://papers.ssrn.com/abstract=311840>.

Emch (2003)

Emch, Eric R. (2003): Price Discrimination via Proprietary Aftermarkets. 2 (1) *Contributions to Economic Analysis & Policy* 4. Available at: <http://www.bepress.com/bejeap/contributions/vol2/iss1/art4>.

EMMS

IBM Electronic Media Management System (EMMS). Available at: <http://www-3.ibm.com/software/data/emms/>.

England, Peinado (2002)

England, Paul/ Peinado, Marcus (2002): Authenticated Operation of Open Computing Devices. In: Batten, Lynn/ Seberry, Jennifer (ed.) (2002): *Information Security and Privacy — 7th Australasian Conference (ACISP 2002)*. Berlin. p. 346.

Erickson (2001)

Erickson, J.S. (April 2001): Information Objects and Rights Management. A Mediation-based Approach to DRM Interoperability. In: *D–Lib Magazine*. Vol. 7. No. 4.

Erickson (2002)

Erickson, J.S. (2002): OpenDRM: A Standards Framework for Digital Rights Expression, Messaging and Enforcement. Hewlett Packard White Paper. Available at: <http://xml.coverpages.org/EricksonOpenDRM200020902.pdf>.

Erickson (2003)

Erickson, John S. (April 2003): Fair Use, DRM, and Trusted Computing. In: 46 (4) *Communications of the ACM* 34.

Ernstthaler (2002)

Ernstthaler, Jürgen et.al. (2002): *Handbuch Urheberrecht und Internet*. Heidelberg.

E–SIGN

US Federal Trade Commission and US Department of Commerce (June 2001): *Electronic Signatures in Global and National Commerce Act (E–SIGN)*. <http://www.ftc.gov/>.

EU Com(88) 72 final.

European Kommission (17. Juni 1988): *Green Paper on Copyright and the Challenge of Technology – Problems in Copyright Calling for Intermediate Action*. Com(88) 72 final.

EU–COM (2002)

Commission of The European Communities (February 2002): *Digital Rights. Background, Systems, Assessment*. Commission Staff Working Paper. Available at: <http://www.politechbot.com/docs/european.commission.drm.030202.pdf>. Last visited: 03 April 2003.

EU-Info-RL

Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft.

European Commission (1992)

Commission of the European Communities: Amended Proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (COM(92) 422 final — SYN 287, 15th October 1992).

European Commission (1999)

European Commission (Nov. 9, 1999): The Development of the Market for Digital Television in the European Union. COM (1999) 540.

European Commission (2002)

Commission of the European Communities: Digital Rights — Background, Systems, Assessment (SEC(2002) 197, 14th February 2002).

European Parliament and Council Directive 98/84/CE

European Parliament and Council Directive 98/84/CE of 20th November 1998 on the legal protection of services based on, or consisting of conditional access. O.J. No. L 320. 28/11/1998 p. 0054-0057.

— F —

Fallenböck (2002/2003)

Fallenböck, M. (Winter 2002/2003): On the Technical Protection of Copyright: The Digital Millennium Copyright Act, the European Community Copyright Directive and Their Anticircumvention Provisions. In: 7 International Journal of Communications Law and Policy. Available at: http://www.ijclp.org/7_2003/pdf/fallenboeck-artikel-ijclp-15-01-03.pdf.

Fallside (2001)

Fallside, D.C. (May 2001): XML Schema Part 0: Primer. W3C Recommendation REC-xmlschema-0-20010502. Available at: <http://www.w3.org/TR/xmlschema-0/>.

Federrath (2002)

Federrath, Hannes (2002): Scientific Evaluation of DRM Systems. In: Conference “Technologische, rechtliche und politische Lösungsstrategien im Umgang mit digitalen Gütern vor dem Hintergrund der europäischen Urheberrechtsrichtlinie”.

Fedwa (1996)

Fedwa, C.S. (1996): Business models for Internetpreneurs, Available at: <http://www.gen.com/global/iess/articles/art4.html> 12.06.1996.

Fehr, Gächter (2000)

Fehr, Ernst/ Gächter, Simon (2000): Fairness and retaliation: the economics of reciprocity. In: Journal of Economic Perspectives. 14. 2000. pp. 159–182.

Feigenbaum (2002)

Feigenbaum, J./ Freedman, M./ Sander, T./ Shostack, A. (5th November 2001): Privacy Engineering for Digital Rights Management Systems. In: Sander (2001): pp. 76–105.

- Feigenbaum, Freedman, Sander, Shostack (2001)
 Feigenbaum, Joan/ Freedman, Michael J./ Sander, Tomas/ Shostack, Adam (2001): Privacy Engineering for Digital Rights Management Systems — ACM CCS-8 Workshop DRM. Privacy Engineering for Digital Rights Management Systems. In: Sander (2001): pp. 76–86.
- Feistel (1973)
 Feistel, Horst (May 1973): Cryptography and Computer Privacy. Scientific American. pp. 15–23.
- Feistel (1974)
 Feistel, Horst (March 1974): Block Cypher Cryptographic System. U.S. patent #3,798,359,19.
- Felsenberg (2002)
 Felsenberg, Alexander (12.9.2002): Rede anlässlich der Präsentation des Gutachtens „Anforderungen an die gesetzliche Regulierung zum Schutz digitaler Inhalte unter Berücksichtigung der Effektivität von technischen Schutzmechanismen“. am 12.9.2002 bei der Medienwoche Berlin. Berlin. Last visited: 12.9.2002. Available at:
http://www.dmmv.de/shared/data/doc/2300.004_rede.af.020911.doc
- Felten (2003)
 Felten, Edward (April 2003): A Skeptical View of DRM and Fair Use. 46 (4) Communications of the ACM 57.
- Ferguson (1993)
 Ferguson, Niels (1993): Extensions of single term coins. In: Advances in Cryptology – CRYPTO '93 – 13th Annual International Cryptology Conference. Proceedings.
- Ferguson (2002)
 Ferguson, Niels (30.1.2002): Anti-circumvention regulation and cryptography research. Vortrag am 30.1.2002 auf der II. Digital Rights Management Konferenz am 29. und 30.1.2002 des Forschungsverbunds Datensicherheit im Haus der Wirtschaft. Berlin. Last visited: 30.1.2002. Available at:
http://www.eurubits.de/drm/drm_2002/audio/ferguson.mp3
- Fetscherin (2002)
 Fetscherin, M. (2002): Present State and Emerging Scenarios of Digital Rights Management Systems. Available at:
<http://www.mediajournal.org/modules/pub/view.php/mediajournal-90>.
 Accessed: 2.12.2002.
- Fichte (1971)
 Fichte, Johann Gottlieb (1971): Beweis der Unrechtmäßigkeit des Büchernachdrucks. Ein Räsonnement und eine Parabel (1793). In: *ibid.* Werke. edited by Immanuel Hermann Fichte. Reprint Berlin. Vol. 8.
- Fichte (1987)
 Fichte, Johann Gottlieb (1987): Beweis der Unrechtmäßigkeit des Büchernachdrucks — Ein Räsonnement und eine Parabel. In: *Berlinische Monatszeitschrift* Vol. 21 (1793). Reprinted in: *UFITA* Vol. 106. p. 155.
- Ficsor (1997)
 Ficsor, Mihaly (1997): Copyright for the Digital Era: The WIPO ‚Internet‘ Treaties. In: *Columbia-VLA J. Law & the Arts* 21.

Field (2000)

Field, Corey (2000): Their mater's voice? Recording artists, bright lines and bowie bonds. In: *Journal of the Copyright Society of the USA*.

Fiedler (2002)

Fiedler, Marina (2002): Rahmenbedingungen der Offenheit wirtschaftender Akteure. In: *Working Paper*. Ludwig-Maximilians-Universität München.

Fishburn, Odlyzko, Siders (1997)

Fishburn, P.C./ Odlyzko, A.M./ Siders, R.C. (July 1997): Fixed fee versus unit pricing for information goods: competition, equilibria, and price wars. In: *First Monday*. 2(7). Available at: <http://firstmonday.org/>. Definitive version in: Kahin, B./ Varian, H.R. (2000): *Internet Publishing and Beyond: The Economics of Digital Information and Intellectual Property*. pp. 167–189.

Fisher (2003)

Fisher, Dennis (2003): Trusted Computing Group Forms. In: *eWeek* (08 Apr 2003). Available at: <http://www.eweek.com/2/0,3959,1010138,00.asp>. Last visited: 12 April 2003.

Fitzpatrick (2000)

Fitzpatrick, S. (2000): Copyright imbalance: U.S. and Australian responses to the WIPO Digital Copyright Treaty. In: *E.I.P.R.* No. 5. pp. 214–228.

Flechsigt (2001)

Flechsigt, Norbert P. (2001): CD-Brenner als urhebervergütungspflichtige Geräte. In: *ZUM* 8/9.2001. pp. 656–660.

Foged (2002)

Foged, Terese (2002): U.S. v. EU Anti-Circumvention Legislation: Preserving the Public's Privileges in the Digital Age. In: *24 European Intellectual Property Review Review* 525.

Forum der Rechteinhaber (2001)

Stellungnahme zur Umsetzung der EU-Info-Richtlinie. Last visited: 24.10.2001. Available at: http://www.gema.de/kommunikation/pressemitteilungen/eu_info_richtlinie_pm.shtml

Forum der Rechteinhaber (2002)

Stellungnahme zum Referententwurf für ein Gesetz zur Regelung des Urheberrechts der Informationsgesellschaft.

Forum der Rechteinhaber (2002a)

Forum der Rechteinhaber (7.8.2002): Kreative brauchen klare Rahmenbedingungen in der Informationsgesellschaft Vorschläge der Buch-, Musik- und Filmbranche für eine Novellierung des Urheberrechts. Last visited: 7.8.2002. Available at: <http://www.buchhandel.de/sixcms/detail.php?id=33476>

Forum der Rechteinhaber (2002b)

Forum der Rechteinhaber (10.2002): Stellungnahme des Forums der Rechteinhaber zum Regierungsentwurf für ein Gesetz zum Urheberrecht in der Informationsgesellschaft. Last visited: 1.11.2002. Available at: <http://www.urheberrecht.org/topic/Info-RiLi/st/Forum-RegEntw.pdf>

Fox (1999)

Fox, Barry (1999): The pirate's tale. *NewScientist*. December 1999.

Fox, LaMacchia (2003)

Fox, Barbara L./ LaMacchia, Brian A. (April 2003): Encouraging Recognition of Fair Uses in DRM Systems. In: 46 (4) *Communications of the ACM* 61.

Franck (1998)

Franck, G. (1998): *Ökonomie der Aufmerksamkeit*. München.

Frankel, Tsiounis, Yung (1996)

Frankel, Y./ Tsiounis, Y./ Yung, M. (1996): Indirect discourse proofs: Achieving efficient fair off-line e-cash. In: *Advances in Cryptology – ASIACRYPT '96*.

Frankel, Tsiounis, Yung (1998)

Frankel, Y./ Tsiounis, Y./ Yung, M. (1998): Fair off-line e-cash made easy. In: *Advances in Cryptology – ASIACRYPT '96*.

Franklin, Yung (1993)

Franklin, M./ Yung, M. (1993): Secure and efficient off-line digital money. In: *Proceedings of the twentieth International Colloquium on Automata, Languages and Programming (ICALP 1993)*.

Freier, Karlton, Kocher (1996)

Freier, A.O./ Karlton, P./ Kocher, P.C. (1996): The SSL protocol version 3.0. Internet Draft. November 1996.

Frey (1998)

Frey, Michael G. (1998): Unfairly Applying the Fair Use Doctrine. In: *University of Cincinnati. Law Review* 66.

Friebel (2000)

Friebel, Lars (2000): Smudo vs. Napster: „Da kommt mir die Galle hoch!“. Last visited: 15.08.2000. Available at: <http://www.heise.de/newsticker/data/chr-15.08.00-000/>

Friedman, Kahn, Howe (2000)

Friedman, Batya/ Kahn, Peter H., Jr./ Howe, Daniel C. (2000): Trust Online. In: *Communications of the ACM*. No. 12. Vol. 43. pp. 34–40.

Frohne (1993)

Frohne, SS Renate (1993): Ashaver Fritsch und das Urheberrecht. In: Wadle, Elmar (ed.) (1993): *Historische Studien zum Urheberrecht in Europa*. Berlin.

Fromm (1965)

Fromm, Friedrich Karl (1965): Das neue deutsche Urheberrecht — Fortschritt und Kritik. In: *UFITA*. Vol. 45. p. 50.

Fromm, Nordemann (1998)

Fromm, Friedrich Karl/ Nordemann, Wilhelm (1998): *Urheberrecht*. Stuttgart.

Froomkin (1996)

Froomkin, A.M. (1996): Flood control on the information ocean, living with anonymity, digital cash, and distributed databases. In: *Pittsburgh Journal of Law and Commerce*. (395).

Froomkin (2000)

Froomkin, A.M. (2000): The Death of Privacy? In: *52 Stanford Law Review*. pp. 1461–1543.

Fujisaki, Okamoto (1997)

Fujisaki, E./ Okamoto, T. (1997): Practical escrow cash system. In: *Security Protocols. International Workshop 1996. Proceedings*.

— G —

Gabber, Silberschatz (1996)

Gabber, E./ Silberschatz, A. (1996): *Agora: A Minimal Distributed Protocol for Electronic Commerce*. In: *Proceedings of the Second USENIX Workshop on Electronic Commerce*. November 1996.

Galline, Scotchmer (2002)

Galline, Nancy & Scotchmer, Suzanne (2002): *Intellectual Property: When is it the Best Incentive Mechanism?* In: Jaffe, Adam/ et al. (eds.)(2002): *Innovation Policy and the Economy*. Vol. 2. Cambridge. p. 51.

Gandy (1993)

Gandy Jr., O.H. (1993): *The Panoptic Sort: A Political Economy of Personal Information*. WBoulder.

Ganea (2001)

Ganea, Peter (2001): *Urheberrecht gestern — heute — morgen: Festschrift für Adolf Dietz zum 65. Geburtstag*. München.

Garfinkel (1998)

Garfinkel, Simson L. (November/December 1998): *The Web's Unelected Government*. *Technology Review* 38.

Garnett (2001)

Garnett, Nic (10.12.2001): *Digital Rights Management, Copyright, and Napster*. Available at: <http://www.acm.org/sigs/sigecom/exchanges/issue-2.2/SEE2.2-Garnett.pdf>

Garnett (2002)

Garnett, Nic (30.1.2002): *Models for Collective vs. Individual Royalties*. Abstrakt zum Vortrag am 30.1.2002 auf der II. Digital Rights Management Konferenz am 29. und 30.1.2002 des Forschungsverbunds Datensicherheit im Haus der Wirtschaft. Berlin. Last visited: 30.1.2002. Available at: <http://www.digital-rights-management.de/digi/konferenzen/drm2002/programm/abstract/garnett.htm>

Gavison (1980)

Gavison, R. (1980): *Privacy and the Limits of Law*. In: 89 *Yale Law Journal*. pp. 421–471.

Gehring (2003)

Gehring, Robert A. (2003): *Software Development, Intellectual Property Rights, and IT Security*. 2nd Bournemouth Symposium on Intellectual Property, Bournemouth. In: *Journal of Information, Law & Technology*. Vol. 8. forthcoming 2003. Available at: <http://elj.warwick.ac.uk/jilt/>.

GEMA, VG Wort, VG Bild-Kunst (2002)

Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte, Verwertungsgesellschaft Wort, Verwertungsgesellschaft Bild-Kunst (2002): *Ja zur privaten Kopie. Davon haben alle mehr!* Flyer.

GEMA, VG Wort, VG Bild-Kunst (2002a)

Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte, Verwertungsgesellschaft Wort, Verwertungsgesellschaft Bild-Kunst (11.3.2002): *Start der Initiative „Ja zur privaten Kopie“ der Autorengesellschaften GEMA, VG WORT und VG Bild-Kunst*. Presseinformation. Last visited: 12.12.2002. Available at: http://www.privatkopieren.de/presse/P1_Musikmesse.pdf

GEMA, VG Wort, VG Bild-Kunst (2002b)

Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte, Verwertungsgesellschaft Wort, Verwertungsgesellschaft Bild-Kunst (12.11.2002): Darum JA zur Privaten Kopie. Last visited: 12.11.2002. Available at: http://www.privatkopieren.de/a_zusammenfassung.html

GEMA Satzung

Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte (25./26. Juni 2002): Satzung der GEMA. Last visited: 11.11.2002. Available at: <http://www.gema.de/wirueberuns/satzung.shtml>

GEMA (2001)

Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte (2001): Geschäftsbericht 2001. München. Last visited: 8.8.2002. Available at: <http://www.gema.de/media/de/geschaeftsbericht2001.pdf>

GEMA (2002)

Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte (3.2002): Stellungnahme. In: CDU/CSU-Bundestagsfraktion (2002): pp. 55-58.

GEMA (2002a)

Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte (1.9.2002): Einigung über Urhebervergütung für CD-Brenner. Available at: <http://www.gema.de/kommunikation/pressemitteilungen/pm20020801.shtml>

Gerber (2001)

Gerber, Tim (25.10.2001): Medienbranche legt Vorschläge zum Urheberrecht vor. Last visited: 25.10.2001. Available at: <http://www.heise.de/newsticker/data/tig-25.10.01-000/>

Gerber (2002)

Gerber, Tim (30.04.2002): Druckerindustrie trommelt gegen Urheberabgaben. Last visited: 30.4.2002. Available at: <http://www.heise.de/newsticker/data/tig-30.04.02-000/>

Gerlach (2002)

Gerlach, Tilo (30.1.2002): „Die Rolle der Verwertungsgesellschaften im digitalen Zeitalter“. 2. Digital Rights Management Conference. Berlin. Haus der Wirtschaft. Vortrag gehalten am 30. Januar 2002.

Germon (1986)

Germon, C. (1986): *La normalisation, cle d'un nouvel essor*. Paris. OECD.

Gervais (1998)

Gervais, D.J. (1998): Electronic Rights Management and Digital Identifier Systems. In: 4 Journal of Electronic Publishing. Issue 2. Available at: <http://www.press.umich.edu/jep/04-03/gervais.html>

Geyskens, Gielens, Dekimpe (2002)

Geyskens, I./ Gielens, K./ Dekimpe, M. G. (2002): The Market Valuation of Internet Channel Additions. *Journal of Marketing*. 66. April. 102–119.

GG

Deutscher Bundestag (12.2001): Grundgesetz für die Bundesrepublik Deutschland. December 2001. Berlin.

- Ghosh, Glott, Krieger, Robles, (2002)
 Ghosh, Rishab Aiyer/ Glott, Rüdiger/ Krieger, Bernhard/ Robles, Gregorio (2002): Free/Libre and Open Source Software: Survey and Study. International Institute of Infonomics, Maastricht, The Netherlands and Berlecon Research GmbH, Berlin. Available at: <http://www.infonomics.nl/FLOSS/report/>. Last visited: 12 March 2003.
- Gillmor (2002)
 Gillmor, Steve (2002): Wild horses. Available at: www.infoworld.com. p. 74.
- Gilmore (2001)
 Gilmore, John (2001): What's Wrong With Copy Protection. Available at: <http://www.toad.com/gnu/whatswrong.html>
- Gimbel (1998)
 Gimbel, Mark (1998): Some Thoughts on the Implications of trusted systems for Intellectual Property Law. In: Stanford Law Review. No. 50. p. 1671.
- Ginsburg (1990)
 Ginsburg, Jane C. (1990): A Tale of Two Cities: Literary Property in Revolutionary France and America. In: Tulane Law Review 64.
- Ginsburg (1995)
 Ginsburg, Jane C. (1995): Domestic and International Copyright Issues Implicated in the Compilation of a Multimedia Product. In: 25 Seton Hall L. Review. 101 ff.
- Ginsburg (1996)
 Ginsburg, Jane C. (1996): Putting Cars on the Information Superhighway. In: Hugenholtz (1996).
- Ginsburg (1999)
 Ginsburg, Jane C. (1999): Copyright Legislation for the Digital Millenium. In: Colum.-VLAJ.L. The Arts 23.
- Ginsburg (2000)
 Ginsburg, Jane C. (2000): From Having Copies to Experiencing Works: The Development of an Access Right in U.S. Copyright Law. In: Columbia Law School - Public Law & Legal Theory Working Paper Group. Paper No. 8. New York. Available at: http://papers.ssrn.com/paper.taf?abstract_id=222493.
- Givon, Mahajan, Muller (1995)
 Givon, M./ Mahajan, V./ Muller, E. (1995): Software Piracy: Estimation of Lost Sales and the Impact on Software Diffusion. In: Journal of Marketing. 59. 1. pp. 29-37.
- Gladney (2000)
 Gladney, Henry M. (2000): Didital Intellectual Property, Controversial & International Aspects. In: 24 Colum. — VLA J. L. & Arts 50
- Glassman, Manasse, Abadi, Gauthier, Sobalvarro (1995)
 Glassman, S./ Manasse, M./ Abadi, M./ Gauthier, P./ Sobalvarro, P. (1995): The MilliCent Protocol for Inexpensive Electronic Commerce. In: Fourth International World Wide Web Conference. December 1995.
- gnutella
 Available at: http://www.gnutelladev.com/protocol/gnutella_protocol.html
- Goffart, Steinbeis (2000)
 Goffart, Daniel / Steinbeis, Maximilian (7.9.2000): IT-Branche protestiert gegen Computer-Abgabe. In: Handelsblatt NR. 173. 7.9.2000. Page 4.

Goldenberg, Libai, Muller (2001)

Goldenberg, J./ Libai, B./ Muller, E. (2001): Talk of the Network: A Complex Systems Look at the underlying Process of Word of Mouth. In: *Marketing Letters*. 12. 3. pp. 211-223.

Goldhaber (1997)

Goldhaber, M.H. (1997): The Attention Economy and the Net. Available at: www.firstmonday.dk/issue/issue2_4/goldhaber/. Last visited: 9.1.2002.

Goldhammer, Zerdick (1999)

Goldhammer, K./ Zerdick, A. (1999): *Rundfunk Online — Entwicklung und Perspektiven des Internets für Hörfunk- und Fernsehanbieter*. Berlin.

Goldmann (2001)

Goldmann, Bettina C. (2001): Die kollektive Wahrnehmung musikalischer Rechte in den USA und Deutschland. München.

Goldmann (2001b)

Goldmann, Bettina C. (2001): Die Regulierung der Urheberverwertungsgesellschaften in den USA. Kollektive Wahrnehmung im Konflikt mit dem Wettbewerbsrecht. In: *GRUR Int.* 2001. p. 420.

Goldmann, Liepe (2002)

Goldmann, Bettina/ Liepe, Andreas (2002): Vertrieb von kopiergeschützten Audio-CDs in Deutschland — Urheberrechtliche, kaufrechtliche und wettbewerbsrechtliche Aspekte. In: *ZUM* 2002. 46/5. pp. 362-375.

Goldstein (1997)

Goldstein, Paul (1997): Copyright and Its Substitutes. In: *Journal of the Copyright Society of the USA* 45.

Goldstein (2001)

Goldstein, Jorge A. (Summer 2001): Patenting the Tools of Drug Discovery. *Drug Discovery World* 9.

Gordijn et al. (2000)

Gordijn, J./ et al. (2000): Selling Bits: A matter of Creating Consumer Value. Available at: <http://www.cs.vu.nl/gordijn/selling-bits.pdf>. Accessed: 11.8.2002.

Gordon (1998)

Gordon, Wendy J. (1998): Intellectual Property as Price Discrimination: Implications for Contract. In: *73 Chicago-Kent Law Review* 1367.

Gordon (2002a)

Gordon, Wendy J. (2002): Excuse and Justification in the Law of Fair Use: Commodification and Market Perspectives. In: Elkin-Koren, Niva & Netanel, Neil W. (eds.), *The Commodification of Information*. The Hague. p. 149.

Gordon (2002b)

Gordon, Wendy J. (2002): Market Failure and Intellectual Property: A Response to Professor Lunney. *82 Boston University Law Review* 1031.

Goto (2001)

Goto, Hideaki (2001): Evulation of Tamper-Resistant Software Deviating from Structured Programming Rules. In: Varadharajan, Vijav & Mu, Yi (eds.), *Information Security and Privacy — 6th Australasian Conference (ACISP 2001)*. Berlin. p. 145.

Grassmuck (2002)

Grassmuck, Volker (2002): Das Ende des Allzweck-Computers. Die Datenherren planen die Aufrüstung des Cyberspace zu einer Welt des totalen "Digital Restrictions Management". In: FIFF-Kommunikation. No. 4. Available at: <http://waste.informatik.hu-berlin.de/Grassmuck/Texts/drm-fiffko.html> Last visited: 31 April 2003.

Graumann (1993)

Graumann, M. (1993): Die Ökonomie von Netzprodukten, Zeitschrift für Betriebswirtschaft. 63. 12. 1331-1355.

Grawrock (2002)

Grawrock, David (Sept. 2002): TCPA 1.2 Specification. Available at <http://www.intel.com/idf/us/fall2002/presentations/SFC173PS.pdf>.

Green (2002)

Green, Lucky (2002): Trusted Computing Platform Alliance: The mother(board) of all Big Brothers. Presentation given at DefCon X, 06 Aug 2002. Available at: http://www.cypherpunks.to/TCPA_DEFCON_10.pdf. Last visited: 31 March 2003.

Green (2003)

Green, Andy (Feb. 21, 2003): The Xbox Is a PC. Available at <http://xbox-linux.sourceforge.net/articles.php?aid=20030051051044>.

Green Paper (1988)

Green Paper on Copyright and the Challenge of Technology - Copyright Issues Requiring Immediate Action. Communication from the Commission. COM (88) 172 final. 7 June 1988.

Green Paper (1995)

Green Paper on Copyright and Related Rights in the Information Society. Brussels. 19.07.1995, COM (95) final.

Green Paper (1998)

Green Paper: Combatting Counterfeiting and Piracy in the Single Market. COM (98) 569 final. 15.10.1998.

Green, Bide

Green, Brian/ Bide, Mark: Unique Identifiers: a brief introduction. Book Industry Communication/EDItEUR. Available at: <http://www.bic.org.uk/uniqueid.html>

Greenleaf (1996a)

Greenleaf, G. (1996): Privacy and cyberspace — an ambiguous relationship. In: 3 Privacy Law & Policy Reporter. pp. 88–92.

Greenleaf (1996b)

Greenleaf, G. (1996): Privacy principles — irrelevant to cyberspace? In: 3 Privacy Law & Policy Reporter. pp. 114–119.

Greenleaf (2002)

Greenleaf, G. (2002): IP, Phone Home: The Uneasy Relationship between Copyright and Privacy, illustrated in the Laws of Hong Kong and Australia. In: 32 Hong Kong Law Journal. pp. 35–81.

Greenspan (2003)

Greenspan, Alan (4 April 2003): Market Economies and Rule of Law. Remarks at the 2003 Financial Markets Conference of the Federal Reserve Bank of Atlanta. Sea Island, Georgia. Available at: <http://www.federalreserve.gov/BoardDocs/speeches/2003/20030404/default.htm> Last visited: 04 April 2003.

Griffith (1999)

Griffith, Sean (1998): Internet Regulation Through Architectural Modification: The Property Rule Structure of Code Solutions. In: *Harvard Law Review*. 112. p. 1634. Available at: http://www.harvardlawreview.org/issues/112/7_1634.html Last visited: 09 April 2003.

Guarino, Welty (2000)

Guarino, Nicola/ Welty, Christopher (August 2000): Identity, Unity, and Individuality: Towards a Formal Toolkit for Ontological Analysis. In: *Proceedings of ECAI-2000: The European Conference on Artificial Intelligence*. Amsterdam.

Guibault (2002)

Guibault, Lucie (2002): *Copyright Limitations and Contracts — An Analysis of the Contractual Overridability of Limitations on Copyright*. London.

Günnewig, Hauser, Himmelein (2002)

Günnewig, Dirk / Hauser, Tobias / Himmelein, Gerald (8.2002): Digitale Rechte am Scheideweg. In: *ct 17/2002*. pp. 18-19.

Güth (1995)

Güth, Werner (1995): On ultimatum bargaining experiments — A personal review. In: *Journal of Economic Behavior & Organization*. 27. 1995. pp. 329–344.

Guth, Koeppen (2002)

Guth, S./ Koeppen, E. (September 2002): Electronic Rights Enforcement for Learning Media. In: *Proceedings of the IEEE International Conference on Advanced Learning Technologies (ICALT)*. Kazan/Russia.

Guth, Simon, Zdun (2003)

Guth, S./ Simon, B./ Zdun, U. (January 2003): A Contract and Rights Management Framework Design for Interacting Brokers. In: *Proceedings of the Hawaii International Conference on System Sciences (HICSS)*. Hawaii/USA.

GVL (2002)

Gesellschaft zur Verwertung von Leistungsschutzrechten (27.11.2002): Wer ist und was macht die GVL? Last visited: 27.11.2002. Available at: <http://www.gvl.de/>

GVL Satzung

Gesellschaft zur Verwertung von Leistungsschutzrechten (28.6.2000): *Satzung, Fassung vom 28. Juni 2000*. Hamburg.

GVU, Scharringhausen (2002)

Gesellschaft zur Verfolgung von Urheberrechtsverletzungen / Scharringhausen, Jan D. (24.6.2002): Referentenentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft. Brief an Dr. Pakuscher. Hamburg.

GVU, Tielke (2002)

Gesellschaft zur Verfolgung von Urheberrechtsverletzungen / Tielke, Joachim (24.6.2002): *Umsetzung der EU-Richtlinie zum Urheberrecht in der Informationsgesellschaft*. Brief an Dr. Pakuscher. Hamburg.

— H —

- Haedicke (2001)
 Haedicke, Maximilian (2001): Die Umgehung technischer Schutzmaßnahmen durch Dritte als mittelbare Urheberrechtsverletzung. In: *Ganea* (2001): pp. 349–364.
- Hagel, Singer (1999)
 Hagel, J./ Singer, M. (1999): Unbundling the Corporation. In: *Harvard Business Review* (March–April 1999). pp. 133–188.
- Haitsma, Kalker, Oostveen (2001)
 Haitsma, J./ Kalker, T./ Oostveen, J. (September 19–21, 2001): “Robust Audio Hashing for Content Identification”. International Workshop on Content-Based Multimedia Indexing. Brescia. Italy.
- Halderman (2002)
 Halderman, J.A. (2002): Evaluating New Copy-Prevention Techniques for Audio CD. Available at: <http://www.cs.princeton.edu/jhalderm/papers/drm2002.pdf>. Accessed: 28.11.2002.
- Hand, Roscoe (2000)
 Hand, S./ Roscoe, T. (2000): Mnemosyne: peer-to-peer steganographic storage. In: *Proceedings of the first International Workshop on Peer-to-Peer Systems*.
- Harbaugh, Khemka (2001)
 Harbaugh, R./ Khemka, R. (2001): Does copyright enforcement encourage piracy? Available at: <http://econ.mckenna.edu/papers/2000-14.pdf>. Accessed: 12.04.2002.
- Hardin (1982)
 Hardin, Russell (1982): *Collective action*. Baltimore, MD.
- Harmon (2001)
 Harmon, Amy (2001): The fight to control intellectual property. In: *New York Times*. Tuesday. Nov 13, 2001.
- Harmon (2002)
 Harmon, Amy (2002): Copyright Hurdles Confront Selling of Music on the Internet. In: *New York Times*. 25.09.2002.
- Harmon (2003)
 Harmon, Amy (2003): Recording industry goes after students over music sharing. In: *New York Times*. April 23, 2003.
- Harms (2001)
 Harms, Jörg Menno (23.3.2001): Vortrag zur BITKOM-Pressekonferenz am 23.3.2001 auf der Cebit. Hannover.
- Harms (2002)
 Harms, Jörg Menno (15.3.2002): Vortrag zum BITKOM-Pressegespräch auf der Cebit „Vergütung von Urheberrechten im digitalen Umfeld“. Hannover.
- Harper (2002)
 Harper, Tieffa (2002): Much Ado About the First Amendment — Does the Digital Millennium Copyright Act Impede the Right to Scientific Expression? In: *12 DePaul-LCA Journal of Art & Entertainment Law* 3.

Harris (2000)

Harris, Scott (14.8.2000): The Piano Roll Precedent. Last visited: 26.11.2002. Available at: <http://www.thestandard.com/article/display/0,1151,17416-0,00.html>

Hart (2002)

Hart, Michael (2002): The Copyright in the Information Society Directive: An Overview. In: 24 European Intellectual Property Review. pp. 58–64.

Haug, Weber (2002)

Haug, S./ Weber, K. (2002): Kaufen oder Tauschen? Reziprozität und rationales Handeln bei Tauschvorgängen unter Freunden und in Internet-Tauschbörsen.

Hauser (2003)

Hauser, Tobias (2003): Kontrollverlust. In c't. Vol. 6.

Hauser, Steiner, Waidner (1996)

Hauser, R./ Steiner, M./ Waidner, M. (1996): Micro-payments based on iKP. In: 14th Worldwide Congress on Computer and Communications Security and Protection (SECURICOM '96). June 1996.

Healy (2003)

Healy, J. (2003): Apple to unveil music service. In: Los Angeles Times. April 28. pp. C1, C5.

Hecker (1999)

Hecker, Frank (1999): Setting Up Shop: The Business of Open-Source Software. In: IEEE Software. 16. pp. 45–51.

Heide (2000)

Heide, T. (2000): Access Control and Innovation under the Emerging EU Electronic Commerce Framework. In: 2000 Berkeley Tech. L.J. Vol. 15. No. 3-. p.993-1048.

Heinrich (1994)

Heinrich, J. (1994): Medienökonomie. Vol. 1. Opladen.

Heinrich (1999)

Heinrich, J. (1999): Medienökonomie. Vol. 2. Opladen.

Heker (1998)

Heker, Harald (10.2.1998): Die Nutzung urheberrechtlich geschützter Werke in digitaler Form. Vortrag beim 4. Europäischen Bielefeld Kolloquium 10.–12. Februar 1998. Bielefeld. Last visited: 1.2.2002. Available at: <http://archiv.ub.uni-bielefeld.de/veranstaltungen/1998/bielefeld.kolloquium.4/0024.htm>

Helberger (1999)

Helberger, N. (1999): “Hacking BskyB: The legal protection of conditional access services under European law”. Entertainment Law Review. 1999-5. p. 88. available at <http://www.ivir.nl/Publicaties/helberger/HackingBskyB.html>

Helix DRM

Helix DRM from RealNetworks. Available at: <http://www.realnetworks.com/products/drm/index.html>

Heller, Eisenberg (1998)

Heller, Michael A./ Eisenberg, Rebecca S. (1998): Can Patents Deter Innovation? Anticommons in Biomedical Research. 280 Science 698.

- Hellmuth, Allamanche, Herre, Kastner, Cremer, Hirsch (2001)
 Hellmuth, O./ Allamanche, E./ Herre, J./ Kastner, T./ Cremer, M./ Hirsch, W. (2001): "Advanced Audio Identification Using MPEG-7 Content Description". 111th AES Convention. New York. Preprint 5463.
- Henkel (2002)
 Henkel, Joachim (2002): Open source software from commercial firms — tools, complements, and collective invention. Ludwig–Maximilians–Universität. München.
- Henrich, Smith (1999)
 Henrich, Joseph/ Smith, Natalie (1999): Culture matters in bargaining and co-operation: cross-cultural evidence from Peru. Chile and the U.S. Working Paper 99–027. Ann Arbor MI. Available at:
<http://eres.bus.umich.edu/docs/workpap/wp99-027.pdf>.
- Herley (2002)
 Herley, Cormac (September 2002): Why watermarking is nonsense. In: IEEE Signal Processing Magazine.
- Herreweghen (1996)
 van Herreweghen, E. (1996): Using digital signatures as evidence of authorizations in electronic credit-card payments. In: Research Report 3156. IBM Research. June 1999.
- Herreweghen (2000)
 van Herreweghen, E. (2000): Non-repudiation in SET: Open Issues. In: Financial Cryptography. 4th International Conference (FC 2000). Proceedings.
- Herzberg, Yochai (1997)
 Herzberg, A./ Yochai, H. (1997): Mini-Pay: Charging per click on the web. In: Sixth International Conference on the World-Wide Web. April 1997.
- Hess, Anding, Schreiber (2002)
 Hess, T./ Anding, M./ Schreiber, M. (2002): Napster in der Videobranche? Erste Überlegungen zu Peer-to-Peer-Anwendungen für Videoinhalte. In: Schoder, D./ Fischbach, D./ Teichmann, R. (ed.)(2002): Peer-to-Peer (P2P): Ökonomische, technologische und juristische Perspektiven. Heidelberg. pp. 25-40.
- Hestermeyer, Worley (2002)
 Hestermeyer, Holger P. / Worley, Christa P. (2002): Tagungsbericht: Digital Rights Management 2002. In: CR 5/2002. 392-393.
- Hill (1999)
 Hill, Keith (1999): A Perspective: The Role of Identifiers in Managing and Protecting Intellectual Property in the Digital Age. In: 87 Proceedings of the IEEE 1228.
- Hillig (1986)
 Hillig, Hans-Peter (1986): Die Urheberrechtsnovelle 1985. In: UFITA. Vol. 102. p. 11.
- Hillig (2002)
 Hillig, Hans-Peter (2002): Urheber- und Verlagsrecht: Textausgabe. 9. Ed. Version: 1.7.2002. München.
- Himmelein (2003)
 Himmelein, Gerald: "Palladium" soll weg. Details zu Microsofts Sicherheits-Initiative. In: c't. No. 5. p. 86–88.

Hippel, Katz (2002)

Hippel, Eric von/ Katz, Ralph (2002): Shifting Innovation to Users via Toolkits. 48 *Management Science* 821.

Hoeren (2000)

Hoeren, Thomas (2000): Urheberrecht 2000 — Thesen für eine Reform des Urheberrechts. In: *MMR* 2000. p. 3.

Hoeren (2001)

Hoeren, Thomas (2001): Geräteabgabe im digitalen Kontext. Ein Kurzgutachten für die COMPAQ Deutschland AG. Münster 27.Juni 2001.

Hoeren (2002)

Hoeren, Thomas (2002): Grundzüge des Internetrechts. E-Commerce, Domains, Urheberrecht. 2. Edition. München.

Hoeren (2002a)

Hoeren, Thomas (29.1.2002): DRM und deutsches Urheberrecht. Vortrag auf der II. Digital Rights Management Konferenz am 29. und 30.1.2002 des Forschungsverbunds Datensicherheit im Haus der Wirtschaft. Berlin. Last visited: 30.1.2002. Available at: http://www.eurubits.de/drm/drm_2002/audio/hoeren.mp3

Hoeren (2002b)

Hoeren, Thomas (26.4.2002): Überlegungen zum Entwurf des Gesetzes zur Regelung des Urheberrechts in der Informationsgesellschaft. Beitrag bei der Konferenz: Digitales Urheberrecht. Zwischen „Information Sharing“ und „Information Control“ — Spielräume für das öffentliche Interesse an Wissen? Konferenz der Heinrich Böll Stiftung und des Netzwerks Neue Medien. 26.4.2002. Berlin. Galerie der Heinrich Böll Stiftung. Available at: <http://www.wissensgesellschaft.org/themen/wemgehört/ueberlegungen.html>

Hoeren (2002c)

Hoeren, Thomas (2.10.2002): Stellungnahme zu §52a Regierungsentwurf des Instituts für Informations-, Telekommunikations- und Medienrecht (ITM). Last visited: 2.10.2002. Available at: http://www.urheberrecht.org/topic/Info-RiLi/st/ITM_52a.pdf

Holeweg (2002)

Holeweg, Annette (3.2002): Beiträge im Wortprotokoll der Anhörung vom 16.11.2000. In: *CDU/CSU-Bundestagsfraktion* (2002): pp. 157, 158.

Hollings

Hollings, F.: Consumer broadband and digital television promotion act.

Holm (2000)

Holm, H. (2000): The Computer Generation's Willingness to Pay for Originals when Pirates are Present — A CV study. School of Economics and Management. Lund University. Lund.

Hopper (2000)

Richard Hopper (September 2000): “EBU Project Group P/META — Metadata Exchange Standards”. In: *EBU Technical Review* (September 2000). Available at: http://www.ebu.ch/trev_284-hopper.pdf.

Hopper (2002)

Hopper R. (April 2002): European Broadcasting Union Technical Review — P/Meta — Metadata Exchange Scheme v1.0. Available at: http://www.ebu.ch/trev_290-hopper.pdf.

Houweling (2002)

Houweling, Molly S. van (2002): Cultivating Open Information Platforms: A Land Trust Model. 1 *Journal on Telecommunications and High Technology Law* 309.

Hovenkamp (1993)

Hovenkamp, Herbert (1993): Market Power in Aftermarkets: Antitrust Policy and the Kodak Case. 40 *UCLA Law Review* 1447.

Huang (2002a)

Huang, Andrew (May 26, 2002): Keeping Secrets in Hardware: the Microsoft XBox Case Study. Available at <ftp://publications.ai.mit.edu/ai-publications/2002/AIM-2002-008.pdf>.

Huang (2002b)

Huang, Andrew (2002): The Trusted PC: Skin-Deep Security. In: 35 (10) *IEEE Computer* 103–104.

Hugenholtz

Hugenholtz, Bernt (2000): Contract and Code: What Will Remain of the Public Domain? In: 26 *Brooklyn Journal of International Law* 77.

Hugenholtz (1996)

Hugenholtz, Bernt (ed.)(1996): *The Future of Copyright in a Digital Environment*. The Hague.

Hugenholtz (1999)

Hugenholtz, Bernt (1999): Code as code, or the end of intellectual property as we know it. In: 6 *Maastricht Journal of European and Comparative Law*. pp. 308–318.

Hugenholtz (2000a)

Hugenholtz, Bernt (2000): “Why the copyright directive is unimportant and possibly invalid”. [2000] *E.I.P.R.* p. 499-502.

Hugenholtz (2000b)

Hugenholtz, Bernt (2000): Contract and Code: What Will Remain of the Public Domain? In: 26 *Brooklyn Journal of International Law* 77.

Hugenholtz (2000c)

Hugenholtz, Bernt (ed.)(2000): *Copyright and Electronic Commerce*. The Hague, London, New York.

Hugenholtz (2002)

Hugenholtz, Bernt (30.1.2002): Anti-circumvention regulation and cryptography research. Vortrag am 30.1.2002 auf der II. Digital Rights Management Konferenz am 29. und 30.1.2002 des Forschungsverbunds Datensicherheit im Haus der Wirtschaft. Berlin. Last visited: 30.1.2002. Available at: http://www.eurubits.de/drm/drm_2002/audio/hugenholtz_1.mp3

Hugenholtz, Guibault, van Geffen (2003)

Hugenholtz, P. Bernt/ Guibault, Lucie/ van Geffen, Sjoerd (March 2003): *The Future of Levies in a Digital Environment*. Available at <http://www.ivir.nl/publications/other/DRM%20Levies%20Final%20Report.pdf>.

Hui (2002)

Hui, K.-L. (2002): Piracy and the Legitimate Demand for Recorded Music. Available at: http://www.comp.nus.edu.sg/ipng/research/Piracy_3.pdf. Accessed: 10.08.2002.

Hummel (2002)

Hummel, Volker (29.5.2002): Kampf um die Privatkopie. In: Financial Times Deutschland. Last visited: 29.5.2002. Available at: <http://www.ftd.de/tm/hs/1014399141723.html>

Huppertz (2001)

Huppertz, Marie Thérèse (2002): The Pivotal Role of Digital Rights Management Systems in the Digital World — An analysis of the copyright protection provided for in the 2001 Copyright Directive with a specific emphasis on the protection of the digital rights management systems and their implementation into the national law. In: 3 Computer Law Review International. 04/2002. pp. 105–112.

Hurd (2001)

Hurd, J. (2001): Pay-for-Content Business Models. A Window of Opportunity for Media and Content Companies. In: Flashpoint.

— I —

Iannella (2001)

Iannella, R. (2001): Digital Rights Management (DRM) Architectures. In: D-Lib Magazine. Vol.7.

Iannella (2002)

Iannella, R. (August 2002): Open Digital Rights Language (ODRL) Specification Version 1.1. IPR Systems White Paper. Available at: <http://www.odrl.net/1.1/ODRL-11.pdf>.

IBM (2002)

IBM News (2002): IBM tops U.S. patent list. Available at: <http://www.ibm.com/news/us/2003/01/131.html> Accessed: 16.3.2003.

IBM-EMMS (2002)

IBM Corporation (November 2002): EMMS Software Suite. Technical White Paper. Available at: <http://www.ibm.com/software/data/emms/>.

IDC (2000a)

IDC (2000): Digital Music Subscriptions — Post-Napster Product Formats.

IDC (2000b)

IDC (2000): Music Download and Consumer Perception: Hype, Skepticism, and the Generation Gap. In: IDC Research (2000).

IEEE

IEEE Learning Technology Standards Committee — Learning Object Metadata Working Group. Available at: <http://ltsc.ieee.org/wg12/>.

IEEE (1997a)

IEEE Symposium on Security and Privacy (04–07 June 1997). Proceedings. Oakland, CA. Available at: <http://www.computer.org/proceedings/sp/7828/7828toc.html> Last visited: 28 March 2003.

IETF (2001)

IETF RFC 3188 (Oct 2001): Using National Bibliography Numbers as Uniform Resource Names. Available at: <http://www.ietf.org/rfc/rfc3188.txt?number=3188>.

IFLA (1998)

IFLA (1998): IFLA Study Group on the Functional Requirements for Bibliographic Records — Functional Requirements for Bibliographic Records. Available at: <http://www.ifla.org/VII/s13/frbr/frbr.pdf>.

IFPI (2000)

IFPI (2000): Piracy Report 2000. London.

IFPI (2001)

Deutsche Landesgruppe der IFPI e.V./ Bundesverband der Phonographischen Wirtschaft e.V. (26.10.2001): Musik als geistiges Eigentum. Last visited: 26.10.2001. Available at: <http://www.ifpi.de/jb/2001/jb01e.html>

IFPI (2001a)

Deutsche Landesgruppe der IFPI (31.12.2001): Die EU-Richtlinie zum Urheberrecht in der Informationsgesellschaft. Last visited: 31.12.2001. Available at: <http://www.ifpi.de/recht/re-21.htm>

IFPI (2002)

IFPI (2002): IFPI Music Piracy report.

IFPI (2002a)

Deutsche Landesgruppe der IFPI/ Bundesverband der phonographischen Wirtschaft (3.2002): Stellungnahme. In: CDU/CSU-Bundestagsfraktion (2002): pp. 33-38.

IFPI (2002b)

Deutsche Landesgruppe der IFPI/ Bundesverband der Phonographischen Wirtschaft (2002): Stellungnahme zum Referentenentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft. Hamburg.

IFPI (2002c)

Deutsche Landesgruppe der IFPI/ Bundesverband der Phonographischen Wirtschaft e.V. (24.4.2002): Stellungnahme zum Referentenentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft

IFPI (2002d)

Deutsche Landesgruppe der IFPI e.V./ Bundesverband der Phonographischen Wirtschaft e.V. (5.8.2002): Umgehung von Kopierschutzsystemen wird gesetzlich verboten. Phonoverbände haben wichtigste Forderung durchgesetzt, sehen aber noch weiteren Änderungsbedarf zum Urheberrechtsgesetz. Hamburg. Last visited: 5.8.2002. Available at: <http://www.ifpi.de/news/news-215.htm>

IFPI (2002e)

Deutsche Landesgruppe der IFPI e.V./ Bundesverband der Phonographischen Wirtschaft e.V. (30.9.2002): Digitale Inhalte müssen geschützt werden. Phonoverbände begrüßen Stellungnahme des Bundesrats zum Urheberrecht. Available at: <http://www.ifpi.de/news/news-224.htm>

IFPI, GEMA (2002)

Deutsche Landesgruppe der IFPI/ Bundesverband der phonographischen Wirtschaft./ GEMA (9.4.2002) Die brennenden Probleme der Musikwirtschaft. Bundesjustizministerium legt ersten Gesetzentwurf für eine Lösung vor. Last visited: 9.4.2002. Available at: <http://ifpi.sesoft.de/html/home.shtml>

ifrOSS, Jäger, Kreutzer (2002)

Institut für Rechtsfragen der freien und Open Source Software/ Jäger, Till/ Kreutzer, Till (11.12.2002): Stellungnahme zum Regierungsentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft. München. Last visited: 11.12.2002. Available at: <http://www.urheberrecht.org/topic/Info-RiLi/st/ifross/art25.pdf>

Imfeld (2003)

Imfeld, Cassandra (2003): Playing Fair With Fair Use? The Digital Millennium Copyright Act's Impact on Encryption Researchers and Academicians. In: 8 Communication Law and Policy 111.

Imprimatur (1997)

Esprit Project 20676 of the European Commission (1997): The Imprimatur Business Model. Version 2.

IMS Health Inc. vs. Commission of the European Communities of 6.8.2001 (Case T-184/01). OJ C 303/19 of 27.10.2001.

Institut für Sozialforschung und Kommunikation/ Shandwick Worldwide (2001)
Studie Urheberrechtsschutz & PC-Drucker. Available at: <http://www.druck-gegen-abgaben.de/data/urheberrechtsschutz.drucker.pdf>

Initiative Privatkopie.net (2002)

Initiative Privatkopie.net (17.6.2002): Petition Rettet die Privatkopie. Last visited: 17.6.2002. Available at: http://www.privatkopie.net/index_1.php

Inness (1992)

Inness, J.C. (1992): Privacy, Intimacy, and Isolation. Oxford, N.Y.

Information and Privacy Commissioner of Ontario (2002)

Information and Privacy Commissioner of Ontario (October 2002): Privacy and Digital Rights Management (DRM): An Oxymoron? Available at: <http://www.ipc.on.ca/docs/drm.pdf>.

International Working Group on Data Protection and Telecommunications (2000)

International Working Group on Data Protection and Telecommunications (4th–5th May 2000): Common Position on Privacy and Copyright Management. Available at: http://www.datenschutz-berlin.de/doc/int/iwgdp/ko_en.htm

Irlam (1995)

Irlam, Gordon (1995): Naming. Available at: <http://www.base.com/gordoni/naming.html>

ISAN

Draft ISO 15706: International Standard Audiovisual Number (ISAN). Available at: <http://www.nlc-bnc.ca/iso/tc46sc9/isan/wg1n1.htm>

ISBN (1992)

ISO 2108:1992 International Standard Book Numbering (ISBN). Available at: <http://www.nlc-bnc.ca/iso/tc46sc9/standard/2108e.htm>

ISBN (1998)

ISO 3297:1998 International Standard Serial Number (ISSN). Available at: <http://www.nlc-bnc.ca/iso/tc46sc9/standard/3297e.htm>

ISBN (2002)

ISO (November 2002): Frequently Asked Questions about changes to the ISBN. Available at: <http://www.nlc-bnc.ca/iso/tc46sc9/isbn.htm>

ISMN (1993)

ISO 10957:1993 International Standard Music Number (ISMN). Available at: <http://www.nlc-bnc.ca/iso/tc46sc9/standard/10957e.htm>

ISRC (2001)

ISO 3901:2001 International Standard Recording Code (ISRC). Available at: <http://www.nlc-bnc.ca/iso/tc46sc9/standard/3901e.htm>

ISRN (1997)

ISO 10444:1997 International Standard Technical Report Number (ISRN). Available at: <http://www.nlc-bnc.ca/iso/tc46sc9/standard/10444e.htm>

ISTC

International Standard Text Code — ISTC — Draft ISO 21047. Available at: <http://www.nlc-bnc.ca/iso/tc46sc9/wg3.htm>

ISWC (2001)

ISO 15707:2001 International Standard Musical Work Code (ISWC). Available at: <http://www.nlc-bnc.ca/iso/tc46sc9/standard/15707e.htm>

— J —

Jaeger, Metzger (2002)

Jaeger, Till/ Metzger, Axel (2002): Open Source Software — Rechtliche Rahmenbedingungen der Freien Software. Munich.

Jaeger, Safford, Franke, (2002)

Jaeger, Trent/ Safford, David/ Franke, Hubertus (2002): Linux Security for the Enterprise: Executive Summary. In: IBM White Paper. Available at: http://www-124.ibm.com/linux/papers/security/les_summary.pdf. Last visited: 3.4.2003.

Jakobsson, Yung (1996)

Jakobsson, M./ Yung, M. (1996): Revokable and versatile electronic money. In: ACM Conference on Computer and Communications Security (CCS'96).

Jakobsson, Yung (1997)

Jakobsson, M./ Yung, M. (1997): Applying anti-trust policies to increase trust in versatile e-money system. In: Financial Cryptography. First International Conference (FC '97). Proceedings.

Jakobsson, MRaihi, Tsiounis, Yung (1999)

Jakobsson, M./ MRaihi, D./ Tsiounis, Y./ Yung, M. (1999): Electronic payments: Where do we go from here? In: Secure Networking – CQRE '99. International Exhibition and Congress, Düsseldorf. Proceedings.

Jarecki, Odlyzko (1997)

Jarecki, S./ Odlyzko, A. (1997): An efficient micropayment system based on probabilistic polling. In: Financial Cryptography. First International Conference (FC '97). Proceedings.

Jarillo (1988)

Jarillo, J.C. (1988): On strategic networks. In: Strategic Management Journal. 9. pp. 90–143.

Jarillo (1993)

Jarillo, J.C. (1993): Strategic networks: Creating the borderless organization. Jordan Hill, England.

- Javanović, Annexstein, Berman (2001)
 Javanović, M./ Annexstein, F./ Berman, K. (2001): Scalability issues in large peer-to-peer networks – a case study of gnutella. Technical report. ECECS Department. University of Cincinnati
- Jayant, Noll (1984)
 Jayant, N./ Noll, P. (1984): “Digital Coding of Waveforms”. Englewood Cliffs, NJ. Prentice-Hall.
- Jehoram (2001)
 Jehoram, Herman C. (2001): The Future of Copyright Collecting Societies. In: 23 European Intellectual Property Review 134.
- Johnson (1985)
 Johnson, William R. (1985): The Economics of Copying. In: Journal of Political Economy. Vol. 93. pp. 158- 174.
- Johnson (2002)
 Johnson, C.A. (August 2002): US eCommerce: The Next Five Years. Forrester Research. Inc. Market Research Report.
- Jolls, Sunnstein, Thaler (1998)
 Jolls, Christine/ Sunnstein, Cass R./ Thaler, Richard (1998): A Behavioral Approach to Law and Economics. In: 50 Stanford Law Review 1471.
- Jupiter Research (2001)
 Jupiter Research (2001): Access, activities, and transactions of the online user. New York.
- Jupiter Research (2002)
 Jupiter Research (2002): Jupiter Consumer Survey Report — Online Music in Europe. European Market Forecasts EUF02-V03. Available at: http://www.jupiterdirect.com/reports/mkt_ad/item/0,4061,2351573.1,00.html Accessed: 10.11.2002.
- Jupiter Research (2002a)
 Jupiter Research (2002): Paid Content in Europe — Using Mobile and Alternative Payments for Incremental Revenues. Jupiter. Entertainment & Media. Vol. 1.
- Jupiter Research (2002b)
 Jupiter Research (2002): Interactive Music Marketing — Driving Off-Line Sales by Targeting Fan Types. European Market Forecasts EUF02-C09.
- Jutla, Yung (1996)
 Jutla, C.S./ Yung, M. (1996): PayTree: “Amortized-signature” for flexible MicroPayments. In: Proceedings of Second USENIX Workshop on Electronic Commerce. November 1996.

— K —

- Kagel, Kim, Moser (1996)
 Kagel, John H./ Kim, Chung/ Moser, Donald (1996): Fairness in ultimatum games with asymmetric information and asymmetric payoffs. In: Games and Economic Behavior. 13. 1996. pp. 100-110.
- Kahn, Cerf (1999)
 Kahn, Robert E. Cerf, Vinton G. (1999): What is the Internet (And What Makes It Work). Available at: http://www.cnri.reston.va.us/what_is_internet.html

Kahn, Lyons (2001)

Kahn, Robert E./ Lyons, Patrice A (2001): Representing Value as Digital Objects: A Discussion of Transferability and Anonymity. In: D-lib. Vol. 5. No. 5. May 2001. Available at: <http://www.dlib.org/dlib/may01/kahn/05kahn.html>

Kahn, Wilensky (1995)

Kahn, Robert E./ Wilensky, R. (1995): A Framework for Distributed Digital Object Services. Available at: <http://www.cnri.reston.va.us/home/cstr/arch/k-w.html>

Kalinke (2002)

Kalinke, Ernst W. (2002): Verbandsprofil Geschichte. Last visited: 30.10.2002. Available at: <http://www.bvkamera.org>

Kalker, Linnartz, van Dijk (1998)

Kalker, T./ Linnartz, J.P.M.G./ van Dijk, M. (October 1998): Watermark Estimation through Detector Analysis. In: Int. Conf. on Image Processing, ICIP. Chicago.

Kanellos (2002)

Kanellos, Michael (2002): Intel: Hyperthreading to speed desktops. In: CNET News.com (09 Sep 2002). Available at: <http://news.com.com/2100-1001-957194.html> Last visited: 04 October 2002.

Kang (1998)

Kang, J. (1998): Information Privacy in Cyberspace Transactions. In: 50 Stanford Law Review. pp. 1193–1294.

Kant (1987)

Kant, Immanuel (1987): Von der Unrechtmäßigkeit des Büchernachdrucks. In: Berlinische Monatsschrift. Vol. 5 (1785). Reprinted in: UFITA Vol. 106. p. 137.

Karas (2001)

Karas, Stan (2001): Sony Computer Entertainment, Inc. v. Connectix Corp. In: 16 Berkeley Technology Law Journal 33.

Kastner, Allamanche, Herre, Cremer, Grossmann, Hellmuth (2002)

Kastner, T./ Allamanche, E./ Herre, J./ Cremer, M./ Grossmann, H./ Hellmuth, O. (2002): "MPEG-7 Scalable Robust Audio Fingerprinting". 112th AES Convention. Munich. Preprint 5511.

Katz (2001)

Katz, Eddan Elizafon (2001): Real Networks Inc. v. Streambox Inc. & Universal City Studios Inc. v. Reimerdes. In: 16 Berkeley Tech. L. J. 53. p. 66.

Katz, Shapiro (1985)

Katz, Michael L./ Shapiro, Carl (1985): Network Externalities, Competition, and Compatibility. In: 75 American Economic Review 424.

Katz, Shapiro (1994)

Katz, Michael L./ Shapiro, Carl (1994): Systems Competition and Network Effects. In: 8 (2) Journal of Economic Perspectives 93.

Kelly (1997)

Kelly, Maureen C. (1997): The Role of A&I services in Facilitating Access to the E-Archive of Science. ICSTI Forum. No. 26. pp1-4. Available at: <http://www.icsti.nrc.ca/icsti/forum/fo9711.html#role>.

Kelly (1998)

Kelly, K. (1998): New Rules for the New Economy. In: 10 Radical Strategies for a Connected World. New York.

Kelsey, Schneier (1998)

Kelsey, J./ Schneier, B. (11.1998): The Street Performer Protocol. The Third USENIX Workshop on Electronic Commerce Proceedings. Nov. 1998. Available at: <http://www.counterpane.com/street-performer.html>

Kelsey, Schneier (1998)

Kelsey, John & Schneier, Bruce (1998): Electronic Commerce and the Street Performer Protocol. Proceedings of the 3rd USENIX Workshop on Electronic Commerce. Available at http://www.usenix.org/publications/library/proceedings/ec98/full_papers/schneier/schneier.pdf.

Kemerling (2002)

Kemerling, G (February 2002): A Dictionary of Philosophical Terms and Names. Available at: <http://www.philosophypages.com/dy/>.

Kenny, Korba (2002)

Kenny, Steve/ Korba, Larry (2002): Applying Digital Rights Management Systems to Privacy Rights Management. In: 21 Computers & Security 648.

Kim, Baek, Lee, Suh (2002)

Kim, Hyung-Shin/ Baek, Yunju/ Lee, Heung-Kyu/ Suh, Young-Ho (2002): Robust image watermark using Radon transform and bispectrum invariants. In: Petitcolas, Fabien A. P. (ed.)(2002): Proceedings of the fifth international workshop on information hiding. Noordwijkerhout, Netherlands.

Kinsely (2001)

Kinsely, M. (2001): Even before the Net, information was free. In: C2C (2001) 1. pp. 1-3.

Kirovski, Malvar (2001)

Kirovski, Darko/ Malvar, Henrique (April 2001): Robust covert communication over a public audio channel using spread-spectrum. In: Moskowitz, Ira S. (ed.)(2001): Proceeding of the fourth international workshop on information hiding. Vol. 2137 of lecture notes in computer science. Pittsburgh, Pennsylvania, U.S.A. pp. 354-368.

Kirovski, Malvar, Yacobi (2001)

Kirovski, Darko/ Malvar, Henrique/ Yacobi, Yacov (June 2001): A dual watermarking and fingerprinting system. Technical report MSR-TR-2001-57. Microsoft Research.

Kirovski, Petitcolas (2003)

Kirovski, D./ Petitcolas, F. (2003): Replacement attack on arbitrary watermarking systems. In: Proceedings of the 2002 ACM Workshop on Digital Rights Management.

Kitch (1986)

Kitch, Edmund W. (1986): Patents: monopolies or property rights? In: Research in Law and Economics. 8. 1986. pp. 31-49.

Kitch (1977)

Kitch, Edmund W. (1977): The Nature and Function of the Patent System. In: 20 Journal of Law and Economics 265.

Kitch (2000)

Kitch, Edmund W. (2000): Elementary and Persistent Errors in the Economic Analysis of Intellectual Property. 53 Vanderbilt Law Review 1727.

Klarmann (21.8.2001)

Klarmann, Michael (21.8.2001): Neue Sachlichkeit. Last visited: 21.8.2001. Available at: <http://www.heise.de/tp/deutsch/inhalt/musik/9362/1.html>

Klein (1993)

Klein, Benjamin (1993): Market Power in Antitrust: Economic Analysis after Kodak. In: 3 Supreme Court Economic Review 43.

Klein, Lerner, Kevin (2002)

Klein, Benjamin/ Lerner, Andres V./ Kevin M. Murphy (2002): The Economics of Copyright "Fair Use" in a Networked World. In: American Economic Review. 92 (2). pp.205-208.

Kleinberg (2000)

Kleinberg, J. (2000): Navigation in a small world. In: Nature 406.

Kleinberg (2001)

Kleinberg, J. (2001): Small-world phenomena and the dynamics of information. Advances in Neural Information Processing (NIPS) 14.

Knies (2002)

Knies, Bernhard (2002): Kopierschutz für Audio-CDs — Gibt es den Anspruch auf die Privatkopie? In: ZUM 2002. 46/11. pp. 793-796.

Knies (2003)

Knies, Bernhard (2003): DeCSS — Spiel mir das Lied vom Code. In: ZUM 2003. 47/4. pp. 286-291.

zu Knyphausen-Aufseß, Meinhardt (2002)

zu Knyphausen-Aufseß, D./ Meinhardt, Y. (2002): Ein Ansatz zur Systematisierung und Kategorisierung von Geschäftsmodellen. In: Bieger, Th./ Bickhoff, N./ Caspers, R./ zu Knyphausen-Aufseß, D./ Reding, K. (ed.)(2002): Zukünftige Geschäftsmodelle — Konzepte und Anwendung in der Netzökonomie. Berlin, Heidelberg, pp. 63-90.

Kocher

Kocher, P. et al.: Self-Protecting Digital Content. Available at: <http://www.cryptography.com/resources/whitepapers/SPDC.htm>

Koelman (2000)

Koelman, K.J. (2000): A Hard Nut to Crack: The Protection of Technological Measures. In: 22 European Intellectual Property Review. pp. 272-280.

Koelman, Helberger (2000)

Koelman, Kamiel J./ Helberger, Natali (2000): Protection of Technological Measures. In: Hugenholtz (2000c): pp. 165-227.

Koenen (1999)

Koenen, Rob (February 1999): MPEG4; Multimedia for our time. In: IEEE Spectrum. Vol. 36. No. 2. pp. 26-33. Available at: <http://mpeg.telecomitalia.com/documents/koenen/mpeg-4.htm>

Kohl (1998)

Kohl, Ulrich (September 1998): Secure Container as a Basis for Cryptographically Secured Multimedia Communication. Multimedia and Security Workshop at ACM Multimedia. Bristol. U.K.

Kohler (1880)

Kohler, Josef (1880): Das Autorrecht. Jena.

Kohler (1907)

Kohler, Josef (1907): *Urheberrecht an Schriftwerken und Verlagsrecht*. Stuttgart.

Konstantas, Morin (2000)

Konstantas, D./ Morin, J.-H. (May 2000): Agent-based Commercial Dissemination of Electronic Information. *Computer Networks*. In: *The International Journal of Computer and Telecommunications Networking*. Vol. 32. No. 6. pp. 753-765.

Korba, Kenny (2002)

Korba, L./ Kenny, S. (November 2002): Towards Meeting the Privacy Challenge: Adapting DRM. NRC Research Paper no. 44956. Presented at workshop on "DRM 2002". Washington, DC. Available at: <http://crypto.stanford.edu/DRM2002/KorbaKennyDRM20021.pdf>.

Korobkin (2003)

Korobkin, Russell (2003): Bounded Rationality and Unconscionability: A Behavioral Theory of Policing Form Contracts. In: *University of Chicago Law Review*, forthcoming 2003. Draft available at <http://papers.ssrn.com/abstract=367172>.

KPMG (2002)

KPMG (2002): *The Digital Challenge: Are you Prepared?* Report.

Krasilovsky, Shemel (2000)

Krasilovsky, W. M./ Shemel, S. (2000): *This Business of Music*. 8th edition. New York.

Kreile (1992)

Kreile, Reinhold (1992): Collection and Distribution of the Statutory Remuneration for Private Copying with Respect to Recorders and Blank Cassettes in Germany. 23 *International Review of Industrial Property & Copyright Law* 449.

Kreile, Becker (1997)

Kreile, Reinhold / Becker, Jürgen (1997): Wesen der Verwertungsgesellschaften. In: Moser, Scheuermann (1997): pp. 621-647.

Kreile, Becker (1997a)

Kreile, Reinhold / Becker, Jürgen (1997a): GEMA und GVL. In: Moser, Scheuermann (1997): pp. 663-679.

Kreile (1999)

Kreile, Reinhold (1999): Die Zusammenarbeit der Verwertungsgesellschaften unter der Aufsicht des Deutschen Patent- und Markenamtes. In: *GRUR* 1999. Vol. 10. pp. 885-889

Kreile (2002)

Kreile, Reinhold (26.6.2002): Rede des Vorsitzenden des Vorstands Prof. Dr. Reinhold Kreile über das 68. Geschäftsjahr 2001 anlässlich der Mitgliederversammlung am 26. Juni 2002. München. Last visited: 26.6.2002. Available at: http://www.gema.de/kommunikation/reden/kreile_mitgliedervers.shtml

Krempl (2001)

Krempl, Stefan (27.8.2001): Datenschützer warnen Urheberrechtsindustrie. Last visited: 27.8.2001. Available at: <http://www.heise.de/newsticker/data/jk-27.08.01-006/>

Krempl (2002)

Krempl, Stefan (2002): E-Publish or Perish — Der vernetzte Weg zur Freien Wirtschaft. In: *CT* 2002. Vol. 18. pp. 84-86.

Krempl (2002a)

Krempl, Stefan (31.1.2002): IT-Branche sieht sich durch Urheberrechtsabgabe existenziell bedroht. Last visited: 31.1.2002. Available at: <http://www.heise.de/bin/nt.print/newsticker/data/jk-31.01.02-003/?id=9aa76846&todo=print>

Krempl (2002b)

Krempl, Stefan (2002): HP-Forscher wirbt für Allianz von Open-Source-Bewegung und TCPA. In: heise newsticker (28.12.2002). Available at: <http://www.heise.de/newsticker/data/se-28.12.02-003/>. Last visited: 28.12.2002.

Krempl (2002c)

Krempl, Stefan (9.5.2002): Justizministerium fordert neue Verhandlungsrunde zu Urheberabgaben. Last visited: 9.5.2002. Available at: <http://www.heise.de/newsticker/data/anw-09.05.02-000/>

Krempl (2002d)

Krempl, Stefan (12.9.2002): Medienverbände stellen Strategie gegen Raubkopierer vor. Last visited: 12.9.2002. Available at: <http://www.heise.de/newsticker/data/vza-12.09.02-000/>

Krempl (2002e)

Krempl, Stefan (12.9.2002a): Politiker gegen weitere Verschärfung des Urheberrechts. Last visited: 12.09.2002. Available at: <http://www.heise.de/newsticker/data/anw-12.09.02-006/>

Krempl (2002f)

Krempl, Stefan (12.12.2002): Lobbystreit um Kopierfreiheiten bei digitalen Medien verschärft sich. Last visited: 12.12.2002. Available at: <http://www.heise.de/newsticker/data/jk-12.12.02-008/>

Krempl (2003)

Krempl, Stefan (12.3.2003): c't aktuell: Rot-grüner „Kompromiss“ fürs digitale Kopieren. Abgerufen am 11.4.2003. Online in: <http://www.heise.de/ct/aktuell/data/anw-12.03.03-022/>

Kretschmer (2002)

Kretschmer, Martin (2002): The Failure of Property Rules in Collective Administration: Rethinking Copyright Societies as Regulatory Instruments. In: 24 European Intellectual Property Review 126.

Kreutzer (2001)

Kreutzer, Till (2001): Napster, Gnutella & Co.: Rechtsfragen zu Filesharing-Netzen aus der Sicht des deutschen Urheberrechts de lege lata und de lege ferenda — Teil 1. In: GRUR 2001. p. 193.

Kreutzer (2002)

Kreutzer, Till (18.10.2002): Freiheit für Lehre und Wissenschaft nach dem künftigen Urheberrecht?! Last visited: 18.10.2002. Available at: <http://www.heise.de/tp/deutsch/special/copy/13445/1.html>

Krill (2003)

Krill, Paul (2003): Linux boost expected for Trusted Computing scheme. In: InfoWorld (29 January 2003). Available at: http://www.infoworld.com/article/03/01/29/hntcpa_1.html Last visited: 23 March 2003.

Kröber (2000)

Kröber, Christian (2000): Vergütungspflicht für digitales Kopieren bestätigt. In: ZUM 7/2000. pp. 545-551.

Kröger (2001)

Kröger (2001): Anmerkungen zu: OLG Hamburg; Urteil vom 6.4.2000. In: Computer und Recht. 10/2000.

Kroon (2000)

Kroon, Annemique M. E. de (2000): Protection of Copyright Management Information. In: Hugenholtz (2000c): pp. 229–265.

Krueger, Bach (2001)

Krueger, W./ Bach, N. (2001): Geschäftsmodelle und Wettbewerb im e-Business. In: Buchholz, E./ Werner, H. (2001): Supply Chain Solutions — Best Practices im E-Business. Stuttgart. pp. 29–51.

Kuhlen (2001)

Kuhlen, Rainer (8.5.2001): Universal Access: Wem gehört das Wissen? Heinrich-Böll-Stiftung (ed.)(2000): Wem gehört das Wissen? Geistiges Eigentum in Zeiten des Internet. Beiträge einer Tagung der Heinrich-Böll-Stiftung am 20. und 21. Oktober 2000 in Berlin. Berlin. Last visited: 27.12.2002. Available at: http://www.bildung2010.de/gutzuwissen/thesen/thesen_kuhlen.html

Kuhlen (2001a)

Kuhlen, Rainer (11.2001): Gutachten zur Auseinandersetzung um die Wahrung von Ansprüchen aus Urheberrechten bzw. Verwertungsrechten durch Pauschalanabgaben auf ICT-Geräte vs. Abrechnung nach individualisierter Inanspruchnahme durch den Einsatz technischer Maßnahmen wie Digital Rights Management. Konstanz.

Kuhlen (2002)

Kuhlen, Rainer (26.4.2002): über die Möglichkeit eines informationsethischen Diskurses über geistiges Eigentum in der Informationsgesellschaft und der Chancen der Umsetzung seiner Argumente in politisch-rechtliche Kodifizierungen. Beitrag bei der Konferenz: Digitales Urheberrecht. Zwischen Information Sharing und „Information Control“ — Spielräume für das öffentliche Interesse an Wissen? Konferenz der Heinrich Böll Stiftung und des Netzwerks Neue Medien. 26.4.2002. Berlin. Galerie der Heinrich Böll Stiftung. Available at: <http://www.wissensgesellschaft.org/themen/wemgehoert/informationsethik.html>

Kulturrat (1998)

Deutscher Kulturrat (29.9.1998): Urheber- und Leistungsschutzrecht in der Informationsgesellschaft. Last visited: 29.9.1998. Available at: <http://www.kulturrat.de/aktuell/Stellungnahmen/urheber.htm>

Kulturrat (2000)

Deutscher Kulturrat (7.9.2000): Deutscher Musikrat, der Rat für Darstellende Künste, die Deutsche Literaturkonferenz, der Kunstrat. Last visited: 7.9.2000. Available at: <http://www.kulturrat.de/themen/presse-urhh-07-09-00.htm>

Kulturrat (2002)

Deutscher Kulturrat (19.4.2002): Stellungnahme des Deutschen Kulturrates zum Referentenentwurf für ein „Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft“. Available at: <http://www.kulturrat.de/aktuell/Stellungnahmen/urheberrecht-infogesellschaft.htm>

Kulturrat (2002a)

Deutscher Kulturrat (6.-8.2002): Zügige Umsetzung der EU-Richtlinie in deutsches Recht. Stellungnahme des Deutschen Kulturrates zum Referentenentwurf für ein „Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft“. In: puk – Politik und Kultur. Ausgabe Juni-August 2002. 17–18.

Kulturrat (2002b)

Deutscher Kulturrat (15.10.2002): Stellungnahme des Deutschen Kulturrates zum Gesetzesentwurf der Bundesregierung für ein „Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft“. Available at: <http://www.kulturrat.de/aktuell/Stellungnahmen/urheberrecht-infogesellschaft-2.htm>

Kumazawa et al. (2000)

Kumazawa, Masayuki/ Kamada, Hironori/ Yamada, Atsushi/ Hoshino, Hiroshi/ Kambayashi, Yahiko/ Mohania, Mukesh (2000): Relationship among Copyright Holders for Use and Reuse of Digital Content. In: Proceedings of the Fifth ACM Conference on Digital Libraries (DL 2000). New York. p. 254.

Kumazawa et al. (2001)

Kumazawa, Masayuki/ Yamada, Atsushi/ Hoshino, Hiroshi/ Kambayashi, Yahiko/ Mohania, Muksh (2001): Representation of Reuse Mechanisms for Digital Work with Multiple Right-Holders. In: Proceedings of the 2001 Symposium on Applications and the Internet — Workshops. SAINT 2001 Workshops. p. 145.

Kundur, Hatzinakos (1998)

Kundur, Deepa/ Hatzinakos, Dimitrios (May 1998): Digital watermarking using multi-resolution wavelet decomposition. Proceedings of the international conference on acoustic. Speech and signal processing (ICASP). Vol. 5. Seattle, Washington, U.S.A. pp. 2969–2972.

Kuri (2003)

Kuri, Jürgen (4.2.2003): IT-Branchenverband wettet gegen Urheber-Pauschale für PCs. Abgerufen am 12.4.2003. Online in: <http://www.heise.de/newsticker/data/jk-04.02.03-008/>

Kuri (2003a)

Kuri, Jürgen (4.2.2003): Urheber-Pauschale für PCs festgelegt [Update]. Abgerufen am 12.4.2003. Online in: <http://www.heise.de/newsticker/data/jk-04.02.03-002/>

Kurth, Clausen (2001)

Kurth, F./ Clausen, M. (2001): “Full-text indexing of very large audio data bases”. 110th AES Convention. Amsterdam. Preprint 5347.

Kutter, Hartung (1999)

Kutter, Martin/ Hartung, Frank (December 1999): Introduction to watermarking techniques. In: Petitcolas, Fabien A. P. / Katzenbeisser, Stefan (eds.)(1999): Information hiding techniques for steganography and digital watermarking.

Kutter, Voloshynovskiy, Herrigel (2000)

Kutter, Martin/ Voloshynovskiy, Sviatoslav/ Herrigel, Alexander (24–26 January 2000): The watermark copy attack. In: Wong, Ping Wah/ Delp, Edward J. (eds.), proceedings of SPIE conference on security and watermarking of multimedia contents II. vol. 3971. San Jose, California. pp. 371–380.

Lagoze (2001)

Lagoze, Carl (January 2001): Keeping Dublin Core Simple: Cross-Domain Discover or Resource Description? In: D-Lib Magazine. Vol. 7. No. 1. doi:10.1045/january2001-lagoze.

Lagoze, Hunter (2001)

Lagoze, Carl/ Hunter, Jane (2.11.2001): The ABC Ontology and Model. In: JoDI. Vol. 2 Issue 2. Available at: <http://jodi.ecs.soton.ac.uk/Articles/v02/i02/Lagoze>.

Lakhani, von Hippel (2000)

Lakhani, Karim/ von Hippel, Eric (2000): How Open Source software works: “Free” user-to-user assistance. Cambridge. MIT Sloan School of Management.

Lampport (1981)

Lampport, L. (1981): Password authentication with insecure communication. In: Communications of the ACM. 24(11). November 1981.

Lamprecht (1784)

Lamprecht, Georg Friedrich (1784): Versuch eines vollständigen Systems der Staatslehre. Vol. 1. Berlin.

Lande (1993)

Lande, Robert H. (1993): Chicago Takes It on the Chin: Imperfect Information Could Play a Crucial Role in the Post-Kodak World. In: 62 Antitrust Law Journal 193.

Landes, Posner (1989)

Landes, William M./ Posner, Richard A. (1989): An Economic Analysis of Copyright Law. Available at: <http://cyber.law.harvard.edu/ipcoop/89land1.html>

Landesbeauftragter für den Datenschutz Mecklenburg-Vorpommern (2003)

Landesbeauftragter für den Datenschutz Mecklenburg-Vorpommern (March 31, 2003): TCPA, Palladium und DRM. Available at: <http://www.datenschutz.mvnet.de/informat/tcpa/tcpa.pdf>.

Langelaar, Lagendijk, Biemond (1998)

Langelaar, Gerrit C./ Lagendijk, Reginald L./ Biemond, Jan (8–11 September 1998): Removing spatial spread-spectrum watermarks by non-linear filtering. In: Proceedings of the 9th European signal processing conference (EU-SIPCO’98). Island of Rhodes, Greece. pp. 2281–2284.

Langelaar, van der Lubbe, Lagendijk (1997)

Langelaar, Gerrit C./ van der Lubbe, Jan C.A./ Lagendijk, Reginald L. (February 1997): Robust labeling methods for copy protection of images. In: Sethin, Ishwar K./ Jain, Ramesh C. (eds.) (1997): Proceedings of the SPIE conference on storage and retrieval for image and video database V. Vol. 3022. San Jose. California, U.S.A. pp. 298–309.

Lanham (1994)

Lanham, R.A. (1994): The Economics of Attention. Available at: www.sunsite.berkeley.edu/ARL/Proceedings/124/ps2econ.html 04.04.2001.

Lasica (15.6.2001)

Lasica, J.D. (15.6.2001): Preventing Content from Being Napsterized: New technologies target theft of online intellectual property. Available at: <http://www.llrx.com/features/napster.htm>

- Laudon, Traver (2002)
Laudon K./ Traver C. (2002): Online Content Providers: Digital Media. Person Education.
- Lehner (2002)
Lehner, Franz (Dec. 8, 2002): Xbox Security Concept. Available at: <http://xbox-linux.sourceforge.net/articles.php?aid=2002341141734>.
- Lejeune (2001)
Lejeune (2001): Der E-Commerce-Vertrag nach amerikanischem Recht. Cologne.
- Lemley (1997)
Lemley, Mark A. (1997): The Economics of Improvement in Intellectual Property Law. In: 75 Texas Law Review 989.
- Lemley (2002)
Lemley, Mark A. (2002): Intellectual Property Rights and Standard Setting Organizations. In: 90 California Law Review 1889.
- Lemley, McGowan (1998)
Lemley, Mark A./ McGowan, David (1998): Legal Implications of Network Economic Effects. In: 86 California Law Review 479.
- Lemos (2003)
Lemos, Robert (2003): Tech titans team for “trusted computing”. In: CNET News (9.4.2003). Available at: <http://news.com.com/2100-1105-996032.html>
Last visited: 11.4.2003.
- Leonard (2003)
Leonard, D. (2003): Facing the music. In: Fortune. March 31. pp. 90–93, 96, 98.
- Lessig (1999)
Lessig, Lawrence (1999): Code and Other Laws of Cyberspace. New York.
- Lessig (2001)
Lessig, Lawrence (2001): The Future of Ideas — The Fate of the Commons in a Connected World. New York.
- Lessig (2001a)
Lessig, Lawrence (2001): The Architecture of Innovation, conference paper. Available at: <http://www.law.duke.edu/pd/papers/lessig.pdf>.
- Leßmann (2001)
Leßmann, Thomas (2001): Verwertungsgesellschaften nach deutschem und europäischem Kartellrecht und deren Herausforderungen im Hinblick auf digitale Techniken. Münster.
- Leupold (1998)
Leupold, Andreas (1998): “Push” und “Narrowcasting” im Lichte des Medien- und Urheberrechts. In: ZUM 1998.
- Leupold, Bräutigam, Pfeiffer (2000)
Leupold, Andreas/ Bräutigam, Peter/ Pfeiffer, Markus (2000): Von der Werbung zur kommerziellen Kommunikation: Die Vermarktung von Waren und Dienstleistungen im Internet. In: WRP 2000.
- Levy (2000)
Levy, Nichelle Nicholes (2000): Method to Their Madness: The Secure Digital Music Initiative, a Law and Economics Perspective. In: 5 Virginia Journal of Law and Technology 12.

Levy (2002)

Levy, Steven (18.3.2002): Locking up your rights. In: *Newsweek*. New York. Mar 18, 2002.

Lichtman (2000)

Lichtman, Douglas (2000): Property Rights in Emerging Platform Technologies. In: 29 *Journal of Legal Studies* 615.

Liebowitz (1985)

Liebowitz, Stanley J. (1985): Copying and Indirect Appropriability: Photocopying of Journals. In: *Journal of Political Economy*. Vol. 94. pp. 822-841.

Liebowitz (2002)

Liebowitz, Stanley J. (2002): Policing Pirates in the Networked Age. Available at: <http://www.cato.org/pubs/pas/pa-438es.html> Accessed: 15.05.2002.

Liebowitz, Margolis (1994)

Liebowitz, Stan J./ Margolis, Stephen E. (1994): Network Externality: An Uncommon Tragedy. 8 (2) *Journal of Economic Perspectives* 133.

Lindsay, Herre (2001)

Lindsay, A./ Herre, J. (July/August 2001): "MPEG-7 and MPEG-7 Audio — An Overview". In: *Journal of the AES*. Vol. 49. No. 7/8. pp. 589-594.

Linnartz, van Dijk (1998)

Linnartz, Jean-Paul M. G./van Dijk, Marten (1998): Analysis of the Sensitivity Attack Against Electronic Watermarks in Images. In: Aucsmith (1998): pp. 258-272.

Lipton, Ostrovsky (1998)

Lipton, R.J./ Ostrovsky, R. (1998): Micro-payments via efficient coin-flipping. In: *Financial Cryptography. Second International Conference (FC'98)*. Proceedings.

Litman (1990)

Litman, Jessica (1990): The Public Domain. In: *Emory Law Journal* 39 (1990). pp. 965 et seq.

Litman (1997)

Litman, Jessica (1997): Reforming Information Law in Copyright's Image. In: *Dayton Law Review* 22.

Liu (2003)

Liu, Joseph P. (2003): The DMCA and the Regulation of Scientific Research. 17 *Berkeley Technology Law Journal* (forthcoming 2003). Draft available at <http://www2.bc.edu/%7Eliujr/scholarship/encryption.doc> (last updated Mar. 20, 2003).

Llorens-Maluquer (1998)

Llorens-Maluquer, Carles (1998): European Responses to Bottlenecks in Digital Pay-TV: Impacts on Pluralism and Competition Policy. In: 16 *Cardozo Arts & Entertainment Law Journal* 557.

Loo (2002)

Loo, P. (March 2002): Digital watermarking using complex wavelets. PhD Thesis. Trinity College. University of Cambridge. England.

Low, Maxemchuk, Paul (1994)

Low, S.H./ Maxemchuk, N.F./ Paul, S. (1994): Anonymous credit cards. In: 2nd ACM Conference on Computer and Communications Security (CCS'94). Proceedings. November 1994.

LTSC (2002)

IEEE Learning Technology Standards Committee [LTSC] (2002): Draft 6.4 of the Learning Object Metadata (LOM). Available at: <http://ltsc.ieee.org/wg12/index.html>

Lucas (2001)

Lucas, André (2001): Le “Triple Test” de l’article 13 d l’accord ADPIC a la lumière du rapport du Groupe Spécial d l’OMC Etas–Unis — Art. 110 (5) de la loi de la droit d’auteur. In: Ganea (2001).

Lunney (2001)

Lunney, Glynn S. (2001): The Death of Copyright — Digital Technology, Private Copying, and the Digital Millennium Copyright Act. In: 87 Virginia Law Review 813.

Lutterbeck, Horns, Gehring (2000)

Lutterbeck, Bernd/ Horns, Axel H./ Gehring, Robert A. Sicherheit in der Informationstechnologie und Patentschutz für Softwareprodukte – ein Widerspruch? [Security in Information Technology and Patent Protection for Software Products: A Contradiction?]. Kurzgutachten für den Bundeswirtschaftsminister. available at: <http://www.sicherheit-im-internet.de/download/Kurzgutachten-Software-patente.pdf>. Last visited: 28 August 2001.

Lyng (2001)

Lyng, Robert (2001): Die Praxis im Musikbusiness. 7. Edition.

Lyon (1994)

Lyon, D. (1994): The Electronic Eye: The Rise of Surveillance Society. Cambridge, Oxford.

Lyon (2002)

Lyon, Gordon E. (Oct. 2002): A Quick–Reference List of Organizations and Standards for Digital Rights Management. National Institute of Standards and Technology Special Publication 500–241. Available at <http://www.itl.nist.gov/div895/docs/NIST241assm.9oct.pdf>. Gaithersburg.

— M —

Machlup, Penrose (1950)

Machlup, Fritz/ Penrose, Edith (1950): The patent controversy in the nineteenth century. In: The Journal of Economic History. 10. 1/1950. pp. 1–29.

Mackay (1991)

Mackay, Wendy E. (1991): Triggers and Barriers to Customizing Software. In: Scott P. Robertson (ed.), Reaching Though Technology — Proceedings of the 8th Conference on Human Factors and Computing Systems 1991. New York. p. 153.

Mahadevan (2000)

Mahadevan, B. (2000): Business Models for Internet–Based E–Commerce: An Anatomy, California Management Review, Vol. 42, No. 4, Summer 2000, pp. 55–69. Available at: <http://unix2.iimb.ernet.in/mahadev/bmodel.pdf>.

Mahajan, Muller, Bass (1990)

Mahajan, V./ Muller, E./ Bass, F. M. (1990): New Product Diffusion Models in Marketing: A Review and Directions for Research. In: Journal of Marketing. 54. 1. 1–26.

Mahajan, Muller, Kerin (1984)

Mahajan, V./ Muller, E./ Kerin, R. (1984): Introduction strategy for new products with positive and negative word of mouth. In: *Management Science*. 30. pp. 1389-1404.

Malone et al. (1987)

Malone, T./ Yates, J./ Benjamin, R. (1987): Electronic markets and hierarchies. In: *Communications of the ACM*. pp. 485-497.

Malvar (1998)

Malvar, H.S. (1998): Enhancing the performance of subband audio coders for speech signals. In: *International Symposium on Circuits and Systems*. Monterey, CA. IEEE. pp. 5/98-5/101.

Malvar (1999)

Malvar, H.S. (1999): A modulated complex lapped transform and its application to audio processing. In: *International Conf. on Acoustics, Speech, and Signal Processing*. Phoenix, AZ. IEEE. pp. 1421-1424.

Marketing Sherpa Inc. (2002)

Marketing Sherpa Inc. (2002): 2nd Annual Selling Subscriptions to Internet Content Summit.

Marks (2002)

Marks, S. (2002): Digital Rights Management and the Bottom Line. Available at: <http://www.cioinsight.com/article2/0,3959,615900,00.asp>. Accessed: 18.08.2002.

Marks, Turnbull (2000)

Marks, Dean S./ Turnbull, Bruce H. (2000): Technical Protection Measures: The Intersection of Technology, Law and Commercial Licenses. In: *22 European Intellectual Property Review*. pp. 198-213.

Marsh (1987)

Marsh, Norman (ed.)(1987): *Public Access to Government-Held Information*. London.

Masson (1996)

Masson, Douglas J. (1996): Fixation on Fixation: Why Imposing Old Copyright Law on New Technology will not work. In: *Indiana LJ* 71.

May, Singer (2001)

May, B./ Singer, M. (2001): Unchained Melody. In: *McKinsey Quarterly*. 1. 1-4.

Mayer-Schönberger (1998)

Mayer-Schönberger, V. (1998): The Internet and Privacy Legislation: Cookies for a Treat? In: *14 Computer Law & Security Report*. pp. 166-174.

McGarvey (2001)

McGarvey, R. (2001): Pay-Per-View's Payback: Cashing in with Content. In: *Econtent* (2001) August 2001. pp. 31-37.

Medvinsky, Neuman (1993)

Medvinsky, G./ Neuman, B.C. (1993): NetCash: A design for practical electronic currency on the Internet. In: *Proceedings of the 1st ACM conference on computer and communications security (CCS '93)*. November 1993.

Mehra (1986)

Mehra, Acham (1986): *Free Flow of Information*. Paris.

Melichar (1983)

Melichar, Ferdinand (1983): Die Wahrnehmung von Urheberrechten durch Verwertungsgesellschaften: am Beispiel der VG Wort. München.

Merges (1996)

Merges, Robert P. (1996): Contracting Into Liability Rules — Intellectual Property Rights and Collective Rights Organizations. In: 84 California Law Review 1293.

Merges, Nelson (1990)

Merges, Robert P./ Nelson, Richard R. (1990): On the Complex Economics of Patent Scope. In: 90 Columbia Law Review 839.

Merritt (2003)

Merritt, Rick (2003): New group aims to secure PCs, PDAs, cell phones. In: iApplianceWeb (09 April 2003). available at: <http://www.iapplianceweb.com/story/OEG20030408S0060>. Last visited: 12 April 2003.

Metadata Registries

ISO/IEC 11179 Information technology — Specification and standardization of data elements. Available at: <http://www.diffuse.org/meta.html>

Metzger (2001)

Metzger, Axel (24.07.2001): Die Privatkopie – vom Aussterben bedroht. Last visited: 24.7.2001. Available at: <http://www.heise.de/tp/deutsch/inhalt/te/9123/1.html>

Meyer (2001)

Meyer, Katrin (2001): Verwertungsgesellschaften und ihre Kontrolle nach dem Urheberrechtswahrnehmungsgesetz. Baden-Baden.

Micali, Rivest (2002)

Micali, S./ Rivest, R.L. (2002): Micropayments revisited. In: Topics in Cryptology – CT-RSA 2002. The Cryptographer’s Track at the RSA Conference 2002. February 2002.

Microsoft — WMRM (2003)

Microsoft Corporation (2003): Understanding how Windows Media Rights Manager Works. Technical White Paper. MSDN Library. Available at: <http://msdn.microsoft.com/library/>.

Microsoft Corp. (2002)

Microsoft Corp. (Aug. 2002): Microsoft “Palladium”: A Business Overview. Available at: <http://www.microsoft.com/presspass/features/2002/jul02/0724palladium wp.asp>.

Microsoft Corp. (2003)

Microsoft Corp. (Feb. 2003): Microsoft Next-Generation Secure Computing Base — Technical FAQ. Available at: <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/news/NGSCB.asp>.

Milgram (1967)

Milgram, S. (1967): The small world problem. Psychology Today 2. pp. 60–67

Miller (2002)

Miller, Ernest (Feb. 28, 2002): Analysis of BNETD and Blizzard. Available at: <http://research.yale.edu/lawmeme/modules.php?name=News&file=article&sid=149>.

Mobile Data Association (2002)

Mobile Data Association (2002): UK Text Message Figure For July Tops 1.35 Billion. Available at:
<http://www.mda-mobiledata.org/resource/hottopics/smsaug02.asp>. Accessed: 24.11.2002

Moe, Fader (2002)

Moe, W. W./ Fader, P. S. (2002): Using Advance Purchase Orders to Forecast New Product Sales. In: *Marketing Science*. 21. 3. 347-364.

Möhring, Nicolini (2000)

Möhring, Philipp/ Nicolini, Käte (2000): *Urheberrechtsgesetz. Gesetz über Urheberrecht und verwandte Schutzrechte*. München.

Möller (1986)

Möller, Margret (1986): *Die Urheberrechtsnovelle '85. Entstehungsgeschichte und verfassungsrechtliche Grundlagen*. Heidelberg.

Monti (2002)

Monti, Mario (2002): Commission of the European Union: Case No COMP/M.3042 — SONY/PHILIPS/INTERTRUST. Regulation (EEC) No 4064/89 Merger Procedure. SG (2002) D/233491/233492. Available at:
http://europa.eu.int/comm/competition/mergers/cases/decisions/m3042_en.pdf. Last visited: 21.4.2003.

Moon (2002)

Moon, Y. (2002): Online Music Distribution in a Post-Napster World. In: *Case Study at Harvard Business School*.

Moore (1989)

Moore, Brian Cecil Joseph (1989): *An introduction to the psychology of hearing*. Third edition. London, England.

Mori (1990)

Mori, R. (1990): Superdistribution: The Concept and the Architecture. In: *The Transactions of the IEICE*. E73. No. 7.

Morrell (8.1.2001):

Morrell, Philippa J.K. (8.1.2001): IFPI Position Paper for the W3C DRM Workshop 22/23 January 2001. Last visited: 8.1.2001. Available at:
<http://www.w3.org/2000/12/drm-ws/pp/ifpi-morrell.html>

Moser (2002)

Moser, Petra (2002): *Determinants of Innovation — New Evidence from 19th Century World Fairs*. In: Sloan School at MIT.

Moser, Scheumann (1997)

Moser, Rolf / Scheumann, Andreas (1997): *Handbuch der Musikwirtschaft*. Starnberg, Berlin.

MPEG-2 Audio (1995)

ISO/IEC ISO/IEC 13818-3:1995. Information technology (October 1995): *Generic coding of moving pictures and associated audio information — Part 3: Audio*.

MPEG-2 IPMP (2002)

ISO/IEC JTC 1/SC 29/WG11 N5061. Klagenfurt. July 2002. This is the current version of the MPEG-2 IPMP Extensions specification. Available at:
http://mpeg.telecomitalia.com/working_documents.htm#MPEG-2.

MPEG-4 Overview (2002)

ISO/IEC JTC1/SC29/WG1/ N4668: Overview of the MPEG-4 Standard, March 2002. Available at: <http://mpeg.telecomitalia.com/standards/mpeg-4/mpeg-4.htm>

MPEG-4 IPMP (2002)

Text of ISO/IEC 14496-1:2001/FPDAM3 and Text of ISO/IEC 14496-13, together comprising the MPEG-4 IPMP Extensions Specification.

MPEG-4 IPMP Hooks (2001)

ISO/IEC 14496-1:2001, The MPEG-4 Systems Specification. Includes version-1 IPMP specification (The “Hooks”) and the MPEG-4 File Format. Related documents are available at: http://mpeg.telecomitalia.com/working_documents.htm#MPEG-4.

MPEG-4 IPMPX (2002)

International Organisation for Standardisation/International Electrotechnical Committee. ISO/IEC 14496-1 FPDAM 3. Information Technology — Coding of Audio-visual Objects — Part 1: Systems. Amendment 3.

MPEG-4 Systems (2001)

International Organisation for Standardisation/ International Electrotechnical Committee (2001): ISO/IEC 14496-1. Information Technology — Coding of Moving Pictures and Audio — Part 1: Systems.

MPEG-7 (2001)

ISO/IEC 15983:2001. Information technology — Coding of moving pictures and audio — Multimedia content description interface (all parts).

MPEG-7 Introduction (2001)

ISO/IEC JTC1/SC29/WG11 (MPEG): “Introduction to MPEG-7”. Document N4032. Singapore. March 2001. Available at: <http://www.csel.it/mpeg>.

MPEG-21 (2003)

ISO/IEC FCD 21000. Information technology — Coding of audiovisual objects — Multimedia framework (all parts).

MPEG-21 DII (2002)

ISO/IEC FCD 21000-3. Information technology — Coding of audiovisual objects — Multimedia framework. Part 6: Digital Item Identification. Final Committee Draft.

MPEG-21 PAT (2003)

ISO/IEC WD 21000-11. Information technology — Coding of audiovisual objects — Multimedia framework Part 11: Evaluation Methods for Persistent Association Technologies. Working Drafts. A current version can be found at: http://mpeg.telecomitalia.com/working_documents.htm#MPEG-21.

MPEG-21 RDD (2003)

ISO/IEC FCD 21000-6. Information technology — Coding of audiovisual objects — Multimedia framework. Part 6: Rights Data Dictionary. Final Committee Draft.

MPEG-21 REL (2003)

ISO/IEC FCD 21000-5. Information technology — Coding of audiovisual objects — Multimedia framework. Part 6: Rights Expression Language. Final Committee Draft.

MPEG-21 Requirements (2002)

ISO/IEC JTC 1/SC 29/ WG11 (MPEG). MPEG-21 Requirements Version 1.3. Document ISO/IEC JTC 1/SC 29/WG 11/N5232. October 2002.

MPEG-21 Vision, Technology & Strategy (2001)

ISO/IEC TR 21000-1. Information technology — Coding of audiovisual objects — Multimedia framework. Part 1: Vision, Technologies and Strategy.

Mueller (2001)

Mueller, Janice M. (2001): No “Dilettante Affair”: Rethinking the Experimental Use Exception to Patent Infringement for Biomedical Research Tools. In: 76 Washington Law Review 1.

Mühlbauer (2001)

Mühlbauer, Peter (17.8.2001): Äußerungen von Peter Mühlbauer zum Thema Geräteabgaben trotz Kopierverbot? Chat / Expertengespräch am 17. 8. 2001, 15 bis 16 Uhr. Last visited: 6.11.2002. Available at: <http://www.heise.de/chat/archiv/01/08/17/archiv.shtml>

Mulligan, Burstein (2002)

Mulligan, Deirdre K./ Burstein, Aaron (2002): Implementing Copyright Limitations in Rights Expression Languages. Available at: http://crypto.stanford.edu/DRM2002/mulligan_burstein_acm_drm_2002.doc. In: Conference Proceeding provided at 2002 ACM Workshop on Digital Rights Management. November 2002. The Wyndham City Center. Washington DC. pp. 113-127. To appear in: Feigenbaum, Joan (ed.)(2003): Security and Piracy in Digital Rights Management. Berlin. Forthcoming 2003.

Musikverleger-Verband (2002)

Deutscher Musikverleger-Verband (3.2002): Stellungnahme. In: CDU/CSU-Bundestagsfraktion (2002): pp. 38-41.

— N —

Nadan (2002)

Nadan, Christian H. (2002): Open Source Licensing: Virus or Virtue? 10 Texas Intellectual Property Law Journal 349.

Netanel (2003)

Netanel, Neil W. (Mar. 2003): Impose a Noncommercial Use Levy to Allow Free P2P File Sharing. Draft available at: http://www.utexas.edu/law/faculty/nnetanel/Levies_chapter.pdf.

Negroponte (1995)

Negroponte, Nicholas (1995): Being Digital. New York.

Neubauer, Brandenburg, Siebenhaar (2002)

Neubauer, Christian/ Brandenburg, Karlheinz/ Siebenhaar, Frank (October 2002): Technical Aspects of Digital Rights Management Systems. Presented at the 113th Convention of the Audio Engineering Society.

Neubauer, Herre (2000)

Neubauer, C./ Herre, J. (2000): “Advanced Watermarking and its Applications”. 109th AES Convention. Los Angeles. Preprint 5176.

Neuman, Medvinsky (1995)

Neuman, B.C./ Medvinsky, G. (1995): Requirements for network payment: The NetCheque perspective. In: Proceedings of IEEE Computer Communications Conference (COMPCON'95). March 1995.

- Neuschmied, Mayer, Batlle (2001)
 Neuschmied, H./ Mayer, H./ Batlle, E. (2001): "Content-based identification of audio titles on the internet". Wedelmusic 2001. Florence.
- Newman (1999)
 Newman, M. (1999): Small worlds: the structure of social networks. Technical Report 99-12-080. Santa Fe Institute.
- Newman, Watts, Strogatz (2002)
 Newman, M./ Watts, D./ Strogatz, S. (2002): Random graph models of social networks. Proc. Natl. Acad. Sci. USA 99. pp. 2566–2572.
- Nicchiotti, Ottaviano (1998)
 Nicchiotti, Gianluca/ Ottaviano, Ennio (8–11 September 1998): Non-invertible statistical wavelet watermarking. In: Proceedings of the 9th European signal processing conference (EUSIPCO'98). pp. 2289–2292. Island of Rhodes, Greece.
- Nikolaidis, Pitas (1998)
 Nikolaidis, N. / Pitas, I. (May 1998): Robust image watermarking in the spatial domain. In: Signal processing. Vol. 66. No. 3. pp. 385–403. ISSN 0165-1684.
- Nimmer (2000)
 Nimmer, David (2000): a Riff on fair use in the Digital Millennium Copyright Act. University of Pennsylvania Law Review Vol. 148. 673. p. 727.
- NISO (1996)
 NISO Standard — Serial Item and Contribution Identifier — ANSI/NISO Z39.56 — 1996 (Version 2). Available at:
<http://www.niso.org/standards/resources/Z39-56.pdf>.
- NISO (2000)
 NISO (August 2000): Draft Standard — Book Item and Component Identifier. Available at: <http://www.niso.org/pdfs/BICI-DS.pdf>.
- Nissenbaum (1999)
 Nissenbaum, Helen (1999): Can Trust be Secured Online? A Theoretical Perspective. In: *Etica e Politica*. No. 2.
- NIST 500-241
 NIST — NIST Special Publication 500-241. Available at:
<http://www.itl.nist.gov/div895/docs/NIST241assm.9oct.pdf>
- NIST (2002)
 NIST [National Institute of Standards and Technology] (July 2002): Common Criteria Evaluation and Validation Scheme Validation Report: Trusted Computing Platform Alliance (TCPA) Trusted Platform Module Protection Profile Version 1.9.7. Report No. CCEVS-VR-02-0022. Available at: http://niap.nist.gov/cc-scheme/PP_TCPATPMPP_V1.9.7-VR.pdf. Last visited: 28 March 2003.
- N.N. (2000)
 HP will GEMA-Gebühr für CD-Brenner nicht zahlen. Last visited: 11.5.2000. Available at: <http://www.heise.de>
- N.N. (2001)
 Urheberrechtspauschale auf PCs: neue Klage. Last visited: 9.4.2001. Available at: <http://www.akademie.de/news/druckbar.html?id=8628>
- N.N. (2001a)
 Streit um Urheberrechtsabgabe für Kombi-Drucker. Last visited: 24.4.2001. Available at: <http://www.heise.de/newsticker/data/em-24.04.01-000/>

N.N. (2001b)

Music Code Cracker to Speak. Last visited: 14.8.2001. Available at: <http://www.wired.com/news/mp3/0,1285,46067,00.html>

N.N. (2002)

Consumer Benefits of today's digital rights management (DRM) solutions. Available at: <http://www.house.gov/judiciary/80031.PDF>. Accessed: 12.07.2002.

Nokia (2001)

Nokia Mobile Phones (2001): Digital Rights Management and Superdistribution of Mobile Content. White Paper. Available at: <http://www.nokia.com/>.

Nordemann (1985)

Nordemann (1985): Die Urheberrechtsreform 1985. In: GRUR. p. 837.

Nordhaus (1969)

Nordhaus, William D. (1969): Invention, growth and welfare: A theoretical treatment of technological change. Cambridge, MA.

North (1991)

North, Douglass Cecil (1991): Institutions, institutional change and economic performance. 2.A. New York.

North (1999)

North, Douglass C. (1999): Where have we been and where are we going? In: Ben-Ner, Avner/ Putterman, Louis (1999): Economics, Values, and Organization. Cambridge, U.K. 1st Paperback Edition. pp. 491–508.

Novos, Waldman (1984)

Novos, Ian E./ Waldman, M. (1984): The Effects of Increased Copyright Protection: An Analytical Approach. In: Journal of Political Economy. Vol. 92. pp. 236-246.



OASIS

The OASIS rights definition homepage:
<http://www.oasis-open.org/committees/rights/>.

O'Brien (2001)

O'Brien, Jeffrey (Nov. 2001): The Making of the Xbox. Wired 9.11. p. 142.

Octalis (2002)

Octalis, S.A. (June 2002): Custom Digital Rights Language (CDRL). White Paper. Available at: <http://octalis.com/R+D/rd.htm>

Okamoto (1995)

Okamoto, T. (1995): An efficient divisible electronic cash scheme. In: Advances in Cryptology – CRYPTO '95 – 15th Annual International Cryptology Conference, Proceedings.

Okamoto, Ohta (1990)

Okamoto, T./ Ohta, K. (1990): Disposable zero-knowledge authentications and their applications to untraceable electronic cash. In: Advances in Cryptology – CRYPTO '89 – 9th Annual International Cryptology Conference, Proceedings.

Okamoto, Ohta (1992)

Okamoto, T./ Ohta, K. (1992): Universal electronic cash. In: Advances in Cryptology – CRYPTO '91, Proceedings.

Olson (1985)

Olson, Mancur (1985): *Die Logik des kollektiven Handelns — Kollektivgüter und die Theorie der Gruppen*. 2. Edition (1. Edition 1968). Tübingen.

OMA

<http://www.openmobilealliance.org/documents.html>

OMA–DCF

Open Mobile Alliance: DRM Content Format Version 1.0, OMA-Download-DRMCF-v1.0.

OMA–DRM

Open Mobile Alliance: Digital Rights Management Version 1.0, OMA-Download-DRM-v1.0.

OMA–REL

Open Mobile Alliance: Rights Expression Language Version 1.0, OMA-Download-DRMREL-v1.0.

OMA (2003)

Open Mobile Alliance (2003): Overview. Available at: <http://www.openmobilealliance.com/docs/OMA%20public%20overview.pdf>. Accessed: 16 Mars 2003.

O'Mahony, Peirce, Tewari (1997)

O'Mahony, D./ Peirce, M./ Tewari, H. (1997): *Electronic Payment Systems*. In: Artech House.

Online Publishers Association (2002)

Online Publishers Association (2002): *Online Paid Content — U.S. Market Spending Report*.

OPIMA

The Open Platform Initiative for Multimedia Access (OPIMA) version 1.0 Specification. Available at: <http://www.cselit.it/ufv/leonardo/opima/torino00/spec11.zip>.

OpenEBook

The OpenEBook Presentation format specification, current version at time of writing at: <http://www.openebook.org/oebps/oebps1.2/index.htm>

Ordovery, Willig (1978)

Ordovery, Janusz A./ Willig, Robert D. (June 1978): *On the Optimal Provision of Journals qua Sometimes Shared Goods*. In: *American Economic Review* – Vol. 68 (3). pp. 324-338.

Ó Ruanaidh, Dowling, Boland (1996)

Ó Ruanaidh, J.J.K./ Dowling, W.J./ Boland, F.M. (September 1996): *Phase watermarking of digital images*. In: *Proceedings of the international conference on image processing (ICIP 1996)*. pp. 215–218.

O'Reilly (1999)

O'Reilly, Tim (1999): *Lessons From Open Source Software Development*. In: *Communications of the ACM*. No. 4. Vol. 42. pp. 33–37.

Ortelli (2002)

Ortelli, Paul (2002): *Talk at Intel Developer Forum Fall 2002*. Available at: <http://www.intel.com/pressroom/archive/speeches/ortellini20020909.html> Last visited: 31 March 2003.

Orwat (2002)

Orwat, C. (2002): Innovationsbedingungen des E-commerce — der elektronische Handel mit digitalen Produkten. Available at: <http://www.tab.fzk.de/de/projekt/zusammenfassung/hp-8.pdf> Accessed: 10.06.2002.

Osborne (2002)

Osborne, Andrew (2002): Business data in the supply chain; part 1: auto ID; Does radio signal the end of the line for bar codes? E.cominfo.net. Available at: <http://www.ecominfo.net/supplychaindata/index2.html>

Ostrom (1990)

Ostrom, Elinor (1990): Governing the commons: the evolution of institutions for collective action. New York.

Ott (2003a)

Ott, Amon (2003): Sicherheits-Architektur. Die Modelle des Linux-Sicherheitssystems Rule Set Based Access Control (RSBAC). In: Linux Magazin. No. 3. pp. 48–54.

Ott (2003b)

Ott, Amon (2003): Wink mit dem Zaunpfahl. Die Modelle des Linux-Sicherheitssystems Rule Set Based Access Control (RSBAC). In: Linux Magazin. No. 4. pp. 61–67.

— P —

Page et al. (1996)

Page, Stanley R./ Johnsgard, Todd J./ Albert, Uhl/ Allen, C. Dennis (1996): User Customization of a Word Processor. In: Tauber, Michael J. (ed.)(1996): Proceedings of the Conference on Human Factors in Computing Systems 1996. New York. p. 340.

Palmer (2001)

Palmer, Sean B. (2001): New URI Schemes: 99% Harmful. Available at: <http://infomesh.net/2001/09/urischemes/>.

Paskin (1999)

Paskin, Norman (1999): Toward Unique Identifiers. In: Proceedings of the IEEE, 87 (no. 7) July 1999. pp. 1208–1227. Available at: <http://www.ieee.org/organizations/pubs/proceedings/intro.html>

Paskin (2001)

Paskin, Norman (June 2002): Towards a Rights Data Dictionary — Identifiers and Semantics at work on the net. imi insights. Available at: <http://www.epsltd.com/IMI/IMI.htm>

Patalong (2002)

Patalong, F. (2002): Was hat Sharman mit KaZaA vor? In: Spiegel Online. 1.10.2002.

Pearson (2003)

Pearson, Siani (ed.)(2003): Trusted Computing Platforms — TCPA Technology in Context. Upper Saddle River.

Pearson, Balacheff, Chen, Plaquin, Proudler (2003)

Pearson, Siani/ Balacheff, Boris/ Chen, Liqun/ Plaquin, David/ Proudler, Graeme (2003): Trusted Computing Platforms. TCPA Technology in Context. Prentice Hall PTR. Upper Saddle River, NJ.

Pedersen (1997)

Pedersen, T.P. (1997): Electronic payments of small amounts. In: Security Protocols, International Workshop 1996, Proceedings.

Peirce (2000)

Peirce, M. (2000): Multi-Party Electronic Payments for Mobile Communications. In: PhD thesis, University of Dublin, Trinity College, Department of Computer Science. October 2000.

Persson (2000)

Persson, Christian (25.11.2000): Initiative D21 macht Front gegen Copyright-Abgabe. Last visited: 25.11.2000. Available at: <http://www.heise.de>

Petersen, Poupard (1997)

Petersen, H./ Poupard, G. (1997): Efficient scalable fair cash with off-line extortion prevention. In: Information and Communications Security, First International Conference (ICICS'97).

Petitcolas, Anderson, Kuhn (1998)

Petitcolas, F.A.P./ Anderson, R.J./ Kuhn, M.G. (April 1998): Attacks on copyright marking systems. In: Aucsmith (1998): pp. 218–238.

Petitcolas (2000)

Petitcolas, Fabien A. P. (2000): Watermarking schemes evaluation. In: I.E.E.E. Signal Processing. Vol. 17. No. 5. pp. 58–64, September 2000.

Petitcolas et al. (2001)

Petitcolas, Fabien A. P./ et al. (2001): A public automated web-based evaluation service for watermarking schemes: StirMark Benchmark. In: Ping Wah Wong/Delp, Edward J. (eds.): Proceedings of Electronic Imaging 2001, Security and Watermarking of Multimedia Contents. Vol. 4314. San Jose, CA, U.S.A. 22–26 January 2001. The Society for imaging science and technology (I.S.&T.) & the international Society for optical engineering (S.P.I.E.). ISSN 0277-786X.

Petitcolas, Kirovski (2002)

Petitcolas, Fabien A. P./ Kirovski, Darko (13–17 May 2002): Blind pattern matching attack on audio watermarking systems. ICASSP 2002. Orlando. Florida. U.S.A.

Pettauer (2000)

Pettauer, Richard (2000): Die Blitzkarriere von MP3. Reales Musikschaffen Für Einen Virtuellen Markt [Online]. Available at: <http://www.mica.at/mf.pettauer.html> Accessed: 10.10.2000.

Peukert (2002)

Peukert, Alexander (2002): Digital Rights Management und Urheberrecht. In: UFITA 2002/III. p. 689.

PewInternet (2002)

PewInternet (2002): The Broadband difference — How online Americans' behavior changes with high-speed Internet connections at home. Available at: http://www.pewinternet.org/reports/pdfs/PIP_Broadband_Report.pdf. Accessed: 25.9.2002.

Pfeiffer (2001)

Pfeiffer, A. (2001): The Hidden Dangers of Digital Rights Management. Available at: http://www.pfeifferreport.com/trends/ett_DRM.html Accessed: 23.3.2002.

Pfitzmann, Federrath, Kuhn (2002)

Pfitzmann, A./ Federrath, H./ Kuhn, M. (2002): Gutachten Datenpiraterie — Technischer Teil. Available at:
http://www.vpirt.de/aktuelles/gutachten/stud_vpirt_datenspiraterie_120902.pdf.
 Accessed: 05.10.2002.

Pfitzmann, Federrath, Kuhn (13.3.2002)

Pfitzmann, Andreas / Federrath, Hannes / Kuhn, Markus (13.3.2002): Anforderungen an die gesetzliche Regulierung zum Schutz digitaler Inhalte unter Berücksichtigung der Effektivität technischer Schutzmechanismen. Studie im Auftrag des Deutschen Multimediaverbandes(dmmv) e.V. und des Verbandes Privater Rundfunk & Telekommunikation (VPRT) e.V. Finale Version vom 13. März 2002. Dresden, Berlin, Cambridge. Last visited: 13.3.2002. Available at: <http://page.inf.fu-berlin.de/feder/publ/2002/copyrightstudie/PfFK2002Final2002-03-13.pdf>

Pfitzmann, Sieber (2002)

Pfitzmann, Andreas/ Sieber, Ulrich (September 2002): Anforderungen an die gesetzliche Regulierung zum Schutz digitaler Inhalte unter Berücksichtigung der Effektivität von technischen Schutzmechanismen. Gutachten erstellt im Auftrag von VPRT und DMMV. Available at: http://www.dmmv.de/shared/data/zip/2501_006_019_druckversion020904.zip. Last visited: 2.4.2003.

Pfitzmann, Sadeghi (2000)

Pfitzmann, B./ Sadeghi, A.-R. (2000): Self-escrowed cash against user black-mailing. In: *Financial Cryptography, 4th International Conference (FC 2000), Proceedings*.

Pfitzmann, Waidner (1996)

Pfitzmann, B. /Waidner, M. (1996): Properties of payment systems: General definition sketch and classification. In: *IBM Research Report RZ 2823 (#90126) 05/06/96*. IBM Research Division. Zurich. May 1996.

Pfitzmann, Waidner, Pfitzmann (1987)

Pfitzmann, B./ Waidner, M./ Pfitzmann, A. (1987): Rechtssicherheit trotz Anonymität in offenen digitalen Systemen. In: *Computer und Recht*. 3(10).

Pfitzmann, Waidner, Pfitzmann (2000)

Pfitzmann, B./ Waidner, M./ Pfitzmann, A. (2000): Secure and anonymous electronic commerce: Providing legal certainty in open digital systems without compromising anonymity. In: *IBM Research Report RZ 3232 (#93278) 05/22/00*. IBM Research Division. Zurich. May 2000.

Pfitzner (2003)

Pfitzner, Roy (Apr. 2003): TCPA, Palladium und DRM — Technische Analyse und Aspekte des Datenschutzes. Version 1.2. Available at:
<http://www.lda.brandenburg.de/material/tcpa.pdf>.

Pfleeger (1996)

Pfleeger, Charles M. (1996): *Security in Computing*. New York. 2nd edition.

Picard (2000)

Picard, R. (2000): Changing Business Models of Online Content Services. In: *The International Journal on Media Management* (2000) 2. pp. 60–68.

- Pickholtz, Schilling, Milstein (1982)
 Pickholtz, Raymond L./ Schilling, Donald L./ Milstein, Laurence B. (May 1982): Theory of spread-spectrum communications — A tutorial. *IEEE transactions on communications*. Vol. 30. No. 5. pp. 855–884.
- Picot, Reichwald, Wigand (2003)
 Picot, A./ Reichwald, R./ Wigand, R. (2003): *Die grenzenlose Unternehmung: Information, Organisation und Management*. Wiesbaden.
- Picot, Ripperger, Wolff (1996)
 Picot, Arnold/ Ripperger, Tanja/ Wolff, Birgitta (1996): The Fading Boundaries of the Firm: The Role of Information and Communication Technology. In: *Journal of Institutional and Theoretical Economics (JITE)*. 152. 1/1996. pp. 65–79.
- Pilioura (1998)
 Pilioura, T. (1998): Electronic payment systems on open computer networks: A survey. In: *Electronic Commerce Objects* (ed. D. Tsichritzis). Centre Universitaire d'Informatique. University of Geneva. July 1998.
- Piller (1998)
 Piller, F.T. (1998): *Kundenindividuelle Massenproduktion. Die Wettbewerbsstrategie der Zukunft*. München.
- Pindyck, Rubinfeld (2001)
 Pindyck, Robert S./ Rubinfeld, Daniel L. (2001): *Microeconomics*. 5th edition. Upper Saddle River.
- Pinto (1984)
 Pinto, Robert (1984): *La liberté d'information et d'opinion en droit international*. Paris.
- Pipkin (2000)
 Pipkin, Donald L. (2000): *Information Security. Protecting the Global Enterprise*. Prentice Hall PTR. Upper Saddle River, NJ.
- Pitas (1996)
 Pitas, Ioannis (September 1996): A method for signature casting on digital images. In: *Proceedings of international conference on image processing (ICIP 1996)*. pp. 215–218.
- Plant (1934)
 Plant, Arnold (1934): The economic theory concerning patents for inventions. In: *Economica*. 1. February. New Series/1934. pp. 30–51.
- Plura (2002)
 Plura, Michael (24.2002): Der PC mit den zwei Gesichtern. TCPA und Palladium — Schreckgespenster oder Papiertiger. In: *c't*. No. 24. pp. 186–188.
- Plura (2003)
 Plura, Michael (2003): TCPA Inside. Intel erweitert den TCPA-Standard mit "LaGrande". In: *c't*. No. 5. p. 87.
- Podilchuk, Zeng (1997)
 Podilchuk, Christine I./ Zeng, Wenjun (10–13 February 1997): Digital image watermarking using visual models. In: Rogowitz, Bernice E./ Pappas, Thrasyvoulos N. (ed.): *Proceedings of the SPIE conference on human vision and electronic imaging II*. Vol. 3016. San Jose, California, U.S.A. pp. 100–111.

Popper (1972)

Popper, Karl R. (1972): *Objective Knowledge: An Evolutionary Approach*. Oxford.

Porter (1990)

Porter, M. (1990): *The competitive advantage of nations*. New York. pp. 42–43.

Porter (2001)

Porter, M.E. (2001): *Strategy and the Internet*. In: *Harvard Business Review* (March 2001). pp. 63–78.

Posner (2001)

Posner, Richard A. (2001): *Antitrust Law*. 2nd edition. Chicago.

Pourzandi, Haddad, Levert, Zakrzewski, Dagenais (2002)

Pourzandi, Makan/ Haddad, Ibrahim/ Levert, Charles/ Zakrzewski, Miroslav/ Dagenais, Michel (2002): *A Distributed Security Infrastructure for Carrier Class Linux Clusters*. In: *IEEE Cluster 2002* (September 23–26, 2002). Chicago, Illinois. Available at: http://www.cs.concordia.ca/~grad/i_haddad/conf2002.html
Last visited: 9.3.2003.

Poutanen, Hinton, Stumm (1998)

Poutanen, T./ Hinton, H./ Stumm, M. (1998): *NetCents: A Lightweight Protocol for Secure Micropayments*. In: *Proceedings of the 3rd USENIX Workshop on Electronic Commerce*. August 1998.

Powell (2002)

Powell, Richard (2002): *2002 CSI/FBI Computer crime and security survey*. Available at: <http://www.gocsi.com/pdfs/fbi/FBI2002.pdf>.

Preston, Lofton (2002)

Preston, Ethan/ Lofton, John (2002): *Computer Security Publications: Information Economics, Shifting Liability and the First Amendment*. In: *24 Whittier Law Review* 71.

Prietze (21.10.2000)

Prietze, Nicola (21.10.2000): *Elektronisches Publizieren stellt Buchmarkt vor neue Herausforderung* Last visited: 22.10.2000. Available at: <http://www.heise.de/newsticker/data/jk-21.10.00-004>

Pruitt (18.4.2002)

Pruitt, Scarlet (18.4.2002): *Law experts leery of digital-rights solution*. Last visited: 18.4.2002. Available at: <http://www.cnn.com/2002/TECH/industry/04/18/dig.rights.mgmt.idg/index.html>

Punch (2001)

Punch, L. (2001): *The shakeout in online cash*. In: *Credit Card Management*. December 2001.

— R —

Radin (2002a)

Radin, Margaret J. (2002): *Incomplete Commodification in the Computerized World*. In: Elkin-Koren, Niva/ Netanel, Neil W. (eds.) (2002): *The Commodification of Information*. The Hague. p. 3.

Radin (2002b)

Radin, Margaret J. (2002): Online Standardization and the Integration of Text and Machine. In: 70 *Fordham Law Review* 1125 (2002).

Raymond (1998)

Raymond, Eric S. (1998): Homesteading the noosphere. Available at: <http://www.firstmonday.dk/issues/issue3.10/raymond/index.html>

Rayport, J.F./ Sviokla, J.J. (1995)

Rayport, J.F./ Sviokla, J.J. (1995): Exploiting the virtual value chain. In: *Harvard Business Review*. Nov./Dec. 1995. pp. 75–85.

Rehbinder (2002)

Rehbinder, Manfred (2002): *Urheberrecht*. Juristische Kurzlehrbücher. 12. Edition. München.

Reinbothe (2001)

Reinbothe, Jörg (2001): Commentary on the Implementation and Effects of Directive 91/250/EEC on the Legal Protections of Computer Programs. In: Hansen, H. C. (ed.) (2001): *International Intellectual Property Law & Policy*. Vol. 6. Huntington. 2001.

Reinbothe (2001a)

Reinbothe, Jörg (2001): Die EG-Richtlinie zum Urheberrecht in der Informationsgesellschaft In: *GRUR Int.*

Reinbothe (2002)

Reinbothe, Jörg (2002): Die Umsetzung der EU-Urheberrechtsrichtlinie in deutsches Recht. In: *ZUM* 2002. 46/1. pp. 43–51.

Renesse (1998)

van Renesse, Rudolf L. (28–30 January 1998): Verifying versus falsifying banknotes. In: van Renesse, Rudolf L. (ed.) (1998): *proceedings of optical security and counterfeit deterrence techniques II*. Vol. 3314. SPIE. p. 71–85. San Jose, California, U.S.A. The Society for imaging science and technology (IS&T) and the international Society for optical engineering (SPIE).

Report from the European Commission on the Application of Council Directive 93/83/EEC on the Coordination of Certain Rules Concerning Copyright and Rights Related to Copyright Applicable to Satellite Broadcasting and Cable Retransmission. COM (2002) 430 final. 26.7.2002.

Report from the Commission to the Council, the European Parliament and the Economic and Social Committee on the Public Lending Right in the European Union. COM (2002) 502 final. 12.9.2002.

Report from the Commission to the Council, the European Parliament and the Economic and Social Committee on the question of authorship of cinematographic or audiovisual works in the Community. COM (2002) 691 final. 6.12.2002.

Report of Lucas. “Pays d’origine contre territorialité” (to be published as part of the Proceedings of the International Conference of Santiago de Compostela.

Retzer (2002)

Retzer, K. (2002): On the Technical Protection of Copyright. In: 3 *Computer und Recht International*. pp. 134–138.

Ricardo (1817)

Ricardo, D. (1817): *Principles of Economy and Taxation*. London. According to: Waenting, H. (ed.) (1821): *Sammlung sozialwissenschaftlicher Meister*. Vol. 5. David Ricardo: Grundsätze der Volkswirtschaft und Besteuerung. 3rd edition. Jena. pp. 119–144.

Rifkin (2000)

Rifkin, J. (2000): *Access. Das Verschwinden des Eigentums*. Frankfurt am Main.

Rivest (1997)

Rivest, R.L. (1997): Electronic lottery tickets as micropayments. In: *Financial Cryptography, First International Conference 1997 (FC'97), Proceedings*.

Rivest, Shamir (1997)

Rivest, R.L./ Shamir, A. (1997): PayWord and MicroMint: Two simple micropayment schemes. In: *Security Protocols, International Workshop 1996, Proceedings*.

Roberts (1988)

Roberts, Ed B. (January 1988): Managing invention and innovation. In: *Research Technology Management*. 1/1988. pp. 11–29.

Robles, Scheider, Tretkowski, Weber (2001)

Robles, Gregorio/ Scheider, Hendrik/ Tretkowski, Ingo/ Weber, Niels (2001): Who Is Doing It? A research on Libre Software developers. In: TU Berlin, Computers and Society Research Group — Research Paper. Available at: <http://ig.cs.tu-berlin.de/s2001/ir2/ergebnisse/OSE-study.pdf>. Last visited: 24 March 2002.

Rogers (1995)

Rogers, E. M. (1995): *Diffusion of Innovations*. Fourth Edition. New York.

Rome Convention

International Convention for the Protection of Performers. Producers of Phonograms and Broadcasting Organisations of October 26. 1961.

Romer (2002)

Romer, P. (2002): When Should We Use Intellectual Property Rights? In: *American Economic Review* – Vol. 92(2). pp. 213–216.

Rose (1999)

Rose, F. (1999): *The economics, concept, and design of information intermediaries: A theoretic approach*. Heidelberg.

Rosenblatt (2002)

Rosenblatt, Bill (25.11.2002): XMP: The Path to Metadata Salvation? In: *The Seybold Report*. Vol 2. No.16. Available at: <http://www.seyboldreports.com/TSR/subs/0216/html/contentman.html>

Rosenblatt, Trippe, Mooney (2002)

Rosenblatt, Bill/ Trippe, William/ Mooney, Stephen (2002): *Digital Rights Management — Business and Technology*. New York.

Rossnagel, Scholz (2000)

Rossnagel, A./ Scholz, P. (2000): Datenschutz durch Anonymität und Pseudonymität: Rechtsfolgen der Verwendung anonymer und pseudonymer Daten. In: *MultiMedia und Recht*. no. 12. pp. 721–731.

Roth (1995)

Roth, Alvin E. (1995): Bargaining experiments. In: Kagel, J. H./ Roth, A. E. (ed.): *The handbook of experimental economics*. Princeton, NJ. pp. 253–348.

Röttgers (2001)

Röttgers, Janko (23.8.2001): Nach dem Crash ist vor dem Crash. Die Popkomm zwischen Krise und Kampfrhetorik. Last visited: 23.8.2001. Available at: <http://www.heise.de/tp/deutsch/inhalt/musik/9378/1.html>

Rump (1996)

Rump, Niels (1996): Copyright Protection of Multimedia Data: The Multimedia Protection Protocol (MMP). International Convention on Sound Design.

Rump, Herre, Brandenburg, Koller, Allamanche (1999)

Rump, Niels/Herre, Jürgen/Brandenburg, Karlheinz/Koller, Jürgen/Allamanche, Eric (1999): White paper on the Secure Digital Music Initiative (SDMI). Fraunhofer IIS.

Rust, Bide (2000)

Rust, Godfrey/ Bide, Mark (2000): The <indec> Metadata Framework: Principles, model and data dictionary. Available at: <http://www.indec.org/pdf/framework.pdf>.

— S —

Safford (2002a)

Safford, David (Oct. 2002): Clarifying Misinformation on TCPA. Available at: http://www.research.ibm.com/gsal/tcpa/tcpa_rebuttal.pdf.

Safford (2002b)

Safford, David (Oct. 2002): The Need for TCPA. Available at http://www.research.ibm.com/gsal/tcpa/why_tcpa.pdf.

Samarajiva (1997)

Samarajiva, R. (1997): Interactivity As Though Privacy Mattered. In: Agre, P.E./ Rotenberg, M. (eds): Technology and Privacy: The New Landscape. Cambridge, Massachusetts, London. pp. 277–309.

Samson (1966)

Samson, Benvenuto (1966): Das neue Urheberrecht. In: UFITA Vol. 47. p. 1.

Samuelson (1993)

Samuelson, Pamela (1993): Fair use for Computer Programs and Other Copyrightable Works in Digital Form: The Implications of Sony, Galoob and Sega. In: Journal of Intellectual Property 1.

Samuelson (1997)

Samuelson, Pamela (1997): The U.S. Digital Agenda at WIPO. In: Virginia Journal of International Art 37.

Samuelson (1999)

Samuelson, Pamela (1999): Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised. In: 14 Berkeley Technology Law Journal. pp. 504–566.

Samuelson (2001)

Samuelson, Pamela (2001): Anticircumvention Rules: Threat to Science. 293 Science 2028.

Samuelson (2003)

Samuelson, Pamela (April 2003): DRM {and, or, vs.} the Law. 46 (4) Communications of the ACM 41.

- Samuelson, Scotchmer (2002)
 Samuelson, Pamela/ Scotchmer, Suzanne (2002): The Law and Economics of Reverse Engineering. In: 111 Yale Law Journal 1575.
- Sander (2001)
 Sander, Tomas (ed.)(2001): Security and Privacy in Digital Rights Management. Berlin.
- Sander (2002)
 Sander, Tomas (2002): Golden Times for Digital Rights Management? In: Syverson, Paul F. (ed.)(2002): Financial Cryptography 2001. Berlin. p. 64.
- Sander, Ta-Shma (1999)
 Sander, T./ Ta-Shma, A. (1999): On anonymous electronic cash and crime. In: Information Security, Second International Workshop (ISW'99).
- Saniers (2000)
 Saniers (2000). In: The International Journal for Communication Studies. p. 379.
- Savage (1995)
 Savage, Diana Wilkins (March 1995): Protecting intellectual property — A warning to the software industry about patents. Available at: <http://www.redherring.com/mag/issue19/property.html>
- Schack (2001)
 Schack, Haimo (2001): Urheber- und Urhebervertragsrecht. 2nd ed. Tübingen.
- Schack (2001b)
 Schack, Haimo (2001): Private Vervielfältigung von einer rechtswidrigen Vorlage? In: Ganea (2001).
- Schack (2002)
 Schack, Haimo (2002): Schutz digitaler Werke vor privater Vervielfältigung — zu den Auswirkungen der Digitalisierung auf § 53 UrhG. ZUM 7/2002. pp. 497–510.
- Schack (2002b)
 Schack, Haimo (2002): Private Vervielfältigung von einer rechtswidrigen Vorlage? In: Ahrens et.al. (2002): p. 165.
- Schack (2003)
 Schack, Haimo (2003): Dürfen öffentliche Einrichtungen elektronische Archiv anlegen? In: AfP 2003. p. 1.
- Schaefer (2000)
 Schaefer, Martin (29.6.2000): Hindernisse auf dem Weg zu einem legalen Online-Musikmarkt. Last visited: 29.6.2000. Available at: <http://www.ifpi.de/recht/re-25.htm>
- Scharpf (2000)
 Scharf, Fritz W. (2000): Interaktionsformen — Akteurzentrierter Institutionalismus in der Politikforschung. Opladen.
- Schlachter (1995)
 Schlachter, E. (1995): Generating revenues from websites. Available at: <http://www.boardwatch/internet.com/mag/95/jul/bwm39.html> 14.07.1995.
- Schmidt, Schunter, Weber (1998)
 Schmidt, M./ Schunter, M./ Weber, A. (1998): Is electronic cash possible? In: Technischer Bericht Nr. A/03/98. Fachbereich Informatik. Universität des Saarlandes.

Schneider (2000)

Schneider, Fred B. (2000): Enforceable Security Policies. In: ACM Transactions on Information and System Security. No. 1.3. pp. 30–50.

Schneider (2003)

Schneider, Volker (2003): Akteurskonstellationen und Netzwerke in der Politikentwicklung. In: Schubert, Bandelow (2003): pp. 107–146.

Schneier (1996)

Schneier, Bruce (1996): Applied Cryptography. 2nd edition. New York. or. Schneier, Bruce (1996): Angewandte Kryptographie. Addison–Wesley. 1. edition.

Schneier (2001)

Schneier, Bruce (May 15 2001): The Futility of Digital Copy Prevention. CRYPTO–GRAM. Available at: <http://www.counterpane.com/crypto-gram-0105.html>

Schneier (2002)

Schneier, Bruce (2002): National strategy to secure cyberspace. Available at: <http://www.counterpane.com/crypto-gram-0210.html>.

Schoen (2002)

Schoen, Seth (Jul. 5, 2002): Palladium Summary. Available at: <http://vitanuova.loyalty.org/2002-07-05.html>

Schreier (2000)

Schreier, E. (2000): Content out of Control. The Forrester Report. Cambridge.

Schricker (1992)

Schricker, Gerhard (1992): Urheberrecht zwischen Industrie– und Kulturpolitik. In: GRUR 1992. p. 242.

Schricker (1997)

Schricker, Gerhard et.al. (ed.)(1997): Urheberrecht auf dem Weg zur Informationsgesellschaft. Gutachten des Max-Planck-Instituts für ausländisches und internationales Patent-, Urheber- und Wettbewerbsrecht. Baden-Baden.

Schricker (1999)

Schricker, Gerhard (ed.)(1999): Urheberrecht. Kommentar. 2nd edition. München.

Schricker, Dreier, Katzenberger, v. Lewinski (1997)

Schricker, G./ Dreier, T./ Katzenberger, P./ v. Lewinski, S. (1997): Urheberrecht auf dem Weg zum Informationszeitalter. Studie im Auftrag des Bundesjustizministeriums. Baden–Baden.

Schricker, Dreier, Kur (2001)

Schricker, G./ Dreier, T./ Kur (ed.)(2001): Geistiges Eigentum im Dienste der Innovation. Baden–Baden.

Schubert, Bandelow (2003)

Schubert, Klaus / Bandelow, Nils (ed.)(2003): Lehrbuch der Politikfeldanalyse. München, Wien.

Schulzki–Haddouti (2003)

Schulzki–Haddouti, Christiane (2003): Bill Gates: Palladium dient auch dem Urheberschutz. In: heise newsticker (09 March 2003). Available at: <http://www.heise.de/newsticker/data/anw-08.03.03-002/>. Last visited: 31 May 2003.

Schwartz (2000)

Schwartz, Paul M. (2000): Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices. In: *Wisconsin Law Review* 743.

Schwarze (2000)

Schwarze, Jürgen (2000): Rechtsschutz gegen Urheberrechtsverletzung und Wettbewerbsverstöße in grenzüberschreitenden Medien. Baden-Baden.

Schwenk (2002)

Schwenk, Joerg (2002): Sicherheit und Kryptografie im Internet. 1. edition.

Screamer (2001)

Screamer, Beale: (18.10.2001): Microsoft's Digital Rights Management Scheme - Technical Details. Last visited: 1.11.2001. Available at: <http://cryptome.org/ms-drm.htm>

SDMI

Available at: <http://www.sdmi.org>.

Seidel (1993)

Seidel, N. (1993): Rundfunkökonomie: Organisation, Finanzierung und Management von Rundfunkunternehmen. Wiesbaden.

SET (1997a)

MasterCard and Visa. The SET Standard Book 1: Business Description. Available at: www.setco.org. May 1997.

SET (1997b)

MasterCard and Visa. The SET Standard Book 2: Programmer's Guide. Available at: www.setco.org. May 1997.

SET (1997c)

MasterCard and Visa. The SET Standard Book 3: Formal Protocol Definitions. Available at: www.setco.org. May 1997.

Seybold Research (2001)

Seybold Research (2001): Digital Rights Management: Usage, Attitudes and Profile of Users. Foster City. 2001.

Shapiro, Varian (1999)

Shapiro, Carl/ Varian, Hal R. (1999): Information Rules: A Strategic Guide to the Network Economy. Boston, M.A.

Shapiro, Vingralek (2001)

Shapiro, William/ Vingralek, Radek (Nov. 2001): How to Manage Persistent State in DRM Systems. ACM CCS-8 Workshop DRM 2001. Philadelphia, PA. USA.

Shavell, Ypersele (2001)

Shavell, Steven; van Ypersele, Tanguy (2001): Rewards versus intellectual property rights. In: *The Journal of Law and Economics*. XLIV. 2 (October)/2001. pp. 527-543.

Shy (2001)

Shy, Oz (2001): *The Economics of Network Industries*. Cambridge.

Shy, Thisse (1999)

Shy, Oz/ Thisse, Jacques F. (Sommer 1999): A Strategic Approach to Software Protection. In: *Journal of Economics and Management Strategy*. Vol. 8 (2). pp. 163-190.

Sibert, Bernstein, Van Wie (1995)

Sibert, O./ Bernstein, D./ Van Wie, D. (July 1995): Digibox: A self-protecting container for information commerce. In: Proceedings of the 1st USENIX Workshop on Electronic Commerce. New York.

Sibold (2001)

Sibold, Kurt (23.3.2001): Vortrag zur BITKOM-Presskonferenz am 23.3.2001 auf der Cebit. Hannover.

Sieber (2002)

Sieber, Ulrich (12.9.2002): Strafrechtlicher Teil. Gutachten zu den Anforderungen an die gesetzliche Regulierung zum Schutz digitaler Inhalte unter Berücksichtigung der Effektivität technischer Schutzmechanismen. Last visited: 12.9.2002. Available at:
http://www.dmmv.de/shared/data/pdf/2501_006_019_jur_gutachten_020904.pdf

Sietmann (2002)

Sietmann, Richard (2002b): Wissen ist Geld. Urheberschutz, Geistiges Eigentum und die Rechtheverwerter. In: c't 24/2002. pp. 108ff. Alternativ: Last visited: 27.12.2002. Available at: <http://www.heise.de/ct/02/24/108/>

SIIA (2001)

SIIA (2001): Global Software Piracy Report 2000. Available at: <http://www.siia.net/piracy/pubs/piracy2000.pdf>. Accessed: 10.2.2002.

SIIA & KPMG (2001)

SIIA/KPMG (2001): Doesn't Everybody Do it? Internet Piracy Attitudes and Behaviors. Available at: <http://www.siia.net/members/divisions/CONTENT/kmpg.pdf>. Accessed: 10.11.2002.

Sinnreich ISO/IEC ISO/IEC 13818-3:1995. Information technology (October 1995) – Generic coding of moving pictures and associated audio information – Part 3: Audio.(2000)

Sinnreich, A. (2000): Digital Music Subscriptions: Post-Napster Product Formats. Jupiter Study.

Sirbu, Tygar (1995)

Sirbu, M./ Tygar, J.D. (1995): NetBill: An Internet commerce system optimized for network delivered services. In: Proceedings of the IEEE Computer Communications Conference (COMPCON'95).

Sirinelli (2001)

Sirinelli, Pierre (2001): The Scope of the Prohibition on Circumvention of Technological Measures: Exceptions - General Report. ALAI 2001 Congress. *Adjuncts and Alternatives to Copyright*. New York. June 13-17.2001. Available at <http://www.law.columbia.edu/conferences/2001/home.en.html>

Skiera (1999)

Skiera, B. (1999): Wie teuer sollen die Produkte sein? — Preispolitik. In: Albers, S./ Clement, M. et.al. (eds.): E-Commerce — Einstieg, Strategie und Umsetzung im Unternehmen. Frankfurt. pp. 94–108.

Slive, Bernhardt (1998)

Slive, J./ Bernhardt, D. (1998): Pirated for profit. In: Canadian Journal of Economics. October. 886-899.

SMPTE (2001)

Society of Motion Picture and Television Engineers (2001): Specification 335M: Television — Metadata Dictionary Structure.

Smudo (2000)

Smudo (Michael B. Schmidt) (29.11.2000): Musiker sollten mit Musik auch Geld verdienen können. Interview vom 29.11.2000. mit Smudo. Name des Journalisten unbekannt. Last visited: 29.11.2000 Available at: <http://www.heise.de/newsticker/data/chr-29.11.00-002>

Sobel (2003)

Sobel, Lionel S. (forthcoming 2003): DRM As an Enabler of Business Models: ISPs as Digital Retailers. 18 Berkeley Technology Law Journal. Draft available at: <https://www.law.berkeley.edu/institutes/bclt/drm/papers/sobel-drm-btj2003.pdf>.

Sohm (1928)

Sohm, Rudolph/ Mitteis, Ludwig/ Wenger, Leopold (1928): Institutionen. Geschichte und System des römischen Privatrechts. München, Leipzig.

Solages, Traoré (1999)

de Solages, A./ Traoré, J. (1999): An efficient fair off-line electronic cash system with extensions to checks and wallets with observers. In: Financial Cryptography – Third International Conference (FC'99), Proceedings.

Solms, Naccache (1992)

von Solms, S./ Naccache, D. (1992): On blind signatures and perfect crimes. In: Computers & Security. 11(6).

De Soto (2000)

De Soto, Hernando (2000): The Mystery of Capital. Basic Books.

Sowa (2000)

Sowa J. F. (2000): Knowledge Representation: Logical, Philosophical and Computational Foundations. Brooks/Cole.

SPI

Case No. Comp/M3042/Sony/Philips/Intertrust. Available at: http://europa.eu.int/comm/competition/mergers/cases/decisions/m3042_en.pdf.

Spindler (2002)

Spindler, Gerald (2002): Europäisches Urheberrecht in der Informationsgesellschaft. In: GRUR (2002). pp. 105–120.

Spindler (2002b)

Spindler, Gerald (2002): Urheberrecht und Tauschplattformen im Internet. In: JZ 2002. p. 60.

SPIO, Film 20 (2002)

Spitzenorganisation der Filmwirtschaft (SPIO) / Film 20 – Interessengemeinschaft Filmproduktion e.V. (18.4.2002): Stellungnahme zu dem Referentenentwurf Urheberrecht in der Informationsgesellschaft vom 18. März 2002.

SPIO, Film 20 (2002a)

Spitzenorganisation der Filmwirtschaft (SPIO) / Film 20 – Interessengemeinschaft Filmproduktion e.V. (28.8.2002): Ausführliche Stellungnahme vom 28. August 2002. Last visited: 28.8.2002. Available at: http://www.urheberrecht.org/topic/Info-RiLi/st/st_film_regentw_28_08_02.pdf

SPIO, Film 20 (2002b)

Spitzenorganisation der Filmwirtschaft (SPIO) / Film 20 – Interessengemeinschaft Filmproduktion e.V. (28.8.2002a): Kurze Stellungnahme vom 28. August 2002. Last visited: 28.8.2002. Available at:
http://www.urheberrecht.org/topic/Info-RiLi/st/Stellgn_Filmw_2.pdf

SPIO, Film 20 (2002c)

Spitzenorganisation der Filmwirtschaft (SPIO) / Film 20 – Interessengemeinschaft Filmproduktion e.V. (11.2002): Politische Stellungnahme zur Umsetzung der Info-Richtlinie in deutsches Urheberrecht hier: Reaktion auf die Gegenäußerung der Bundesregierung. Last visited: 11.12.2002. Available at:
<http://www.spio.de/Stellungnahme261102.pdf>

Stallings (1999)

Stallings, William (1999): *Cryptography and Network Security. Principles and Practice*. 2nd ed. Upper Saddle River, NJ.

Stallman (1999)

Stallman, Richard M. (1999): *The GNU Operating System and the Free Software Movement*. In: DiBona, Chris/ Ockman, Sam/ Stone, Mark (eds.) (1999): *Open Sources — Voices From the Open Source Revolution*. Sebastopol. p. 53.

Stallman (2002a)

Stallman, Richard M. (2002): *Can You Trust Your Computer?* In: Gay, Joshua (ed.) (2002): *Free Software, Free Society: Selected Essays of Richard M. Stallman*. Boston. p. 115.

Stallman (2002b)

Stallman, Richard M. (2002): *Why You Shouldn't Use the Library GPL for Your Next Library*. Available at: <http://www.fsf.org/philosophy/why-not-lgpl.html> (last modified Oct. 24, 2002).

Steiner, Neuman, Schiller (1988)

Steiner, J.G./ Neuman, C./ Schiller, J.I. (1988): *Kerberos: An authentication service for open network systems*. In: *Proceedings of the Winter 1988 Usenix Conference*. February 1988.

Steinmüller (1993)

Steinmüller, Wilhelm (1993): *Informationstechnologie und Gesellschaft*. Darmstadt.

Stefik (1996)

Stefik, Mark (1996): *Letting Loose the Light: Igniting Commerce in Electronic Publication*. In: Stefik, Mark (1996): *Internet Dreams: Archetypes, Myths, and Metaphors*. Cambridge, MA. pp. 219–253.

Stefik (1997)

Stefik, Mark (1997): *Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge Us to Rethink Digital Publishing*. In: *Berkeley Technology Law Journal*. Vol. 12. No. 1. pp. 137–159. Available at:
<http://www.law.berkeley.edu/journals/btlj/articles/vol12/Stefik/html/reader.html> Last visited: 07 March 2003.

Stefik (1999)

Stefik, Mark (1999): *The Internet Edge. Social, Legal, and Technological Challenges for a Networked World*. Cambridge, MA/ London, UK.

Sterling (1998)

Sterling, J.A.L. (1998): *World Copyright Law*. London.

Stieler (2002)

Stieler, Wolfgang (6.12.2002): eBook-Hacker tritt nicht als Zeuge auf. Last visited: 6.12.2002. Available at: <http://www.heise.de/newsticker/data/wst-06.12.02-002/>

Stoica, Morris, Karger, Kaashoek, Balakrishnan (2001)

Stoica, I./ Morris, R./ Karger, D./ Kaashoek, M.F./ Balakrishnan, H. (2001): CHORD: A scalable peer-to-peer lookup service for internet applications. In: Proceedings of the ACM SIGCOMM 2001 Conference (SIGCOMM-01). pp. 149–160.

Stopper (2002)

Stopper, Martin (2002): Schrankenbestimmungen für Internetwerke. In: Ernthaler, Jürgen et.al. (2002): Handbuch Urheberrecht und Internet. Heidelberg, 207-215.

Sun, Lannom (2002)

Sun, Sam/ Lannom, Larry (July 2002): Handle System Overview. CNRI. Available at: <http://www.ietf.org/internet-drafts/draft-sun-handle-system-10.txt>.

Sun, Reilly, Lannom (2002)

Sun, Sam/ Reilly, Sean/ Lannom, Larry (July 2002): Handle System Namespace and Service Definition. CNRI. Available at: <http://www.ietf.org/internet-drafts/draft-sun-handle-system-def-06.txt>.

Sun, Reilly, Lannom, Petrone (2002)

Sun, Sam/ Reilly, Sean/ Lannom, Larry/ Petrone, Jason (July 2002): Handle System Protocol (Ver 2.1) Specification. CNRI. Available at: <http://www.ietf.org/internet-drafts/draft-sun-handle-system-protocol-03.txt>.

Swanson, Zu, Tewfik (1996)

Swanson, Mitchell D./ Zu, Bin/ Tewfik, Ahmed H. (1996): Robust Data Hiding for Images. In: Proceedings of the 7th digital signal processing workshop (DSP 96). pp. 37–40. Loen, Norway.

Sydow (1993)

Sydow, J. (1993): Strategische Netzwerke: Evolution und Organisation. Wiesbaden.

— T —

Takeyama (1994)

Takeyama, Lisa N. (June 1994): The Welfare Implications of Unauthorized Reproduction of Intellectual Property in the Presence of Demand Network Externalities. In: Journal of Industrial Economics – Vol. 17. pp. 155–166.

Takeyama (1997)

Takeyama, Lisa N. (1997): The Intertemporal Consequences of Unauthorized Reproduction of Intellectual Property. In: Journal of Law and Economics – Vol. 40. pp. 511-522.

Takeyama (2002)

Takeyama, Lisa N. (2002): Piracy, Asymmetric Information, and Product Quality Revelation. Department of Economics. Amherst College. Amherst.

Tam (2003)

Tam, P.-W. (2003): Apple launches online store offering downloadable music. In: The Wall Street Journal. April 29, 2003. p. B8.

Tanaka, Nakamura, Matsui (1990)

Tanaka, K./ Nakamura, Y./ Matsui, K. (1990): Embedding secret information into a dithered multilevel image. In: Proceedings of the IEEE Military Communications Conference. pp. 216–220.

Tang (1995)

Tang, L. (1995): A set of protocol for micropayments in distributed systems. In: Proceedings of the first USENIX Workshop on Electronic Commerce.

Tang (1998)

Tang, Puay (1998): How Electronic Publishers are Protecting against Privacy: Doubts about Technical Systems of Protection. In: The Information Society. Vol. 14. No. 1. pp. 19–31.

Tassey (2000)

Tassey, Gregory (2000): Standardization in Technology–Based Markets. Research Policy. Vol 20. pp. 587–602.

Taylor (1994)

Taylor, L. D. (1994): Telecommunications Demand in Theory and Practice. Dordrecht. Boston. London.

Taylor (2000)

Taylor, Jim (2000): DVD Demystified. 2nd edition. New York.

TCG (2003)

Trusted Computing Group (2003): Frequently Asked Questions. Available at <http://www.trustedcomputinggroup.org/about/faq>.

TCPA (2001)

Trusted Computing Platform Alliance (Sep. 9, 2001): TCPA PC Specific Implementation Specification. Version 1.00. Available at: http://www.trustedcomputing.org/docs/TCPA_PCSpecificSpecification_v100.pdf.

TCPA (2002)

Trusted Computing Platform Association (2002): TCPA Main Specification Version 1.1b.

TCPA (2002a)

Trusted Computing Platform Alliance (Feb. 22, 2002): Main Specification. Version 1.1b. Available at: <http://www.trustedcomputing.org/docs/main%20v1.1b.pdf>.

TCPA (2002b)

Trusted Computing Platform Alliance (Jul. 1, 2002): Trusted Platform Module Protection Profile. Version 1.9.7. Available at: http://www.trustedcomputing.org/docs/TCPA_TPM_PP_1.9.7.pdf.

TCPA (2002c)

Trusted Computing Platform Alliance (Oct. 16, 2002): TCPA Specification/TPM Q&A. Available at: http://www.trustedcomputing.org/docs/TPM-QA_1016021.pdf.

TCPA–QA (2002)

TCPA [Trusted Computing Platform Alliance] (October 2002): TCPA Specification/TPM Q&A. Available at: http://www.trusteddcomputing.org/docs/TPM-QA_1016021.pdf. Last visited: 28.3.2003.

TCPA-Spec (2002)

TCPA [Trusted Computing Platform Alliance] (May 2002): TCPA Main Specification Version 1.1b. Available at: <http://www.trustedcomputing.org/cpaasp4/specs.asp>. Last visited: 28.3.2003.

TCPA-SpecImpl (2001)

TCPA [Trusted Computing Platform Alliance] (September 2001): TCPA PC Specific Implementation Specification Version 1.00. Available at: <http://www.trustedcomputing.org> Last visited: 28.3.2003.

TCPA-TPMProf (2002)

TCPA [Trusted Computing Platform Alliance] (October 2002): TCPA TPM Protection Profile Version 1.9.7. Available at: http://www.trustedcomputing.org/docs/TCPA_TPM_PP_1.9.7.pdf. Last visited: 28.3.2003.

Teece (1998)

Teece, David J. (1998): Capturing value from knowledge assets: The new economy, markets for know-how, and intangible assets. In: *California Management Review*. 40. Jg. 3/1998. pp. 55–79.

Terwangne, Louveaux (1997)

de Terwangne, C./ Louveaux, S. (1997): Data Protection and Online Networks. In: *13 Computer Law & Security Report*. pp. 234–246.

Thurow (1994)

Thurow, N. (1994): Die digitale Verwertung von Musik aus der Sicht von Schallplattenproduzenten und ausübenden Künstlern. In: Becker, Dreier (1994): p. 77.

Theedar (1999)

Theedar, S. (1999): Privacy in photographic images. In: *6 Privacy Law & Policy Reporter*. pp. 75–78.

Thomke, Hippel (2002)

Thomke, Stefan & Hippel, Eric von (April 2002): Customers as Innovators — A New Way to Create Value. *Harvard Business Review* 74.

Thoms (3.2002)

Thoms, Frank (3.2002): Beiträge im Wortprotokoll der Anhörung vom 16.11.2000. In: *CDU/CSU-Bundestagsfraktion (2002)*: pp. 157, 161-162.

Thong, Hong, Tam (2002)

Thong/ Hong/ Tam (2002): Understanding user acceptance of digital libraries: what are the roles of interface characteristics, organizational context, and individual differences? Elsevier Science Ltd. London.

Tien (1999)

Tien, Lee (1999): Publishing Software as a Speech Act. In: *14 Berkeley Tech. L. J.* 629.

Tirkel, Rankin, van Schyndel, Ho, Mee, Osborne (1993)

Tirkel, A./ Rankin, G./ van Schyndel, R. G./ Ho, W./ Mee, N./ Osborne, C. (December 1993): Electronic water mark. In: *Proceedings DICTA 1993*. pp. 666–672.

Tonninger (1998)

Tonninger, Bernhard (1998): Copyright und Urheberrecht im Internet : aktuelle, globale Rechtsentwicklungen unter Berücksichtigung von Datenbanken und Lösungsvorschläge zur Providerhaftung und zur Behandlung neuer Internetphänomene. 1. Edition. Graz.

Tornatzky, Klein (1982)

Tornatzky, L. G./ Klein, K. J. (1982): Innovation Characteristics and Innovation Adoption - Implementation: A Meta-Analysis of Findings. IEEE Transactions on Engineering Management. 29. 1. 28-45.

Touretzky (2000)

Touretzky, D. S. (2000): Gallery of CSS Descramblers. Available at: <http://www.cs.cmu.edu/~dst/DeCSS/Gallery>.

Trampas (2002)

Trampas, A. Kurth (2002): Digital Rights Management: An Overview of the Public Policy Solutions to Protecting Creative Works in a Digital Age. WISE 2002. Kansas State University. Prepared For The Institute of Electrical and Electronics Engineers. Inc. August 2002.

Triplett (2001)

Triplett, J. (2001): CD Copy Protection: Yea or Ne'? Available at: http://www.jamesontriplett.com/Writings/cd_copy_protection.htm Accessed: 19.02.2002.

TRIPS Agreement (1994)

Agreement on Trade-Related Aspects of Intellectual Property Rights, Annex I C of the Marrakesh Agreement Establishing the World Trade Organization of April 15, 1994.

Tschmuck (2000)

Tschmuck, P. (2000): Internetökonomie und Musikwirtschaft. Reales Musikschaffen Für Einen Virtuellen Markt [Online]. Available at: http://www.mica.at/mf_tschmuck_p.html Accessed: 10 October 2000.

TÜViT (2002)

TÜViT (December 2002): Technische Schutzmaßnahmen in Verbindung mit Digital Rights Management Systemen — geeignete Systeme zur individuellen Lizenzierung. Studie im Auftrag der BITKOM Servicegesellschaft mbH. Essen.

Tzovaras, Karagiannis, Strintzis (1998)

Tzovaras, Dimitrios/ Karagiannis, Nikitas/ Strintzis, Michael G. (8–11 September 1998): Robust image watermarking in the subband or discrete cosine transform domain. In: Proceedings of the 9th European Signal Processing Conference (EUSIPCO'98). Island of Rhodes. pp. 2285–2288.

Ulmer (1965)

Ulmer, Eugen (1965): Das neue deutsche Urheberrechtsgesetz. In: UFITA Vol. 45. p. 48.

Ulmer (1971)

Ulmer, Eugen (1971): Elektronische Datenbanken und Urheberrecht. Munich.

Ulmer (1980)

Ulmer, Eugen (1980): Urheber- und Verlagsrecht. 3. Edition. Berlin.

Universität Siegen - Medienzentrum (2002)

Gewährleistung des freien Zugangs für Studium, Lehre und Forschung zur Information in der digitalen Informationsgesellschaft. Stellungnahme zum §52a im Regierungsentwurf vom 31.07.2002 für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft. Unterzeichnet vom Leiter der Medienstelle Dr. Hartmut Simon. Siegen. Last visited: 18.12.2002. Available at: <http://www.urheberrecht.org/topic/Info-RiLi/st/BMJ041002.pdf>

UrhG 22.3.2002

Gesetz über Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz) vom 9. September 1965. Zuletzt geändert durch Gesetz vom 22.3.2002. Zitiert nach: Hillig, Hans-Peter (2002): Urheber- und Verlagsrecht: Textausgabe. 9. neubearbeitete Ausgabe. Stand 1. Juli 2002. München. pp. 3-53.

UrhGRefE 18.3.2002

Bundesministerium der Justiz (18.3.2002): REFERENTENENTWURF für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft. Last visited 18. März 2002. Berlin. Last visited: 20.3.2002. Available at: http://www.urheberrecht.org/topic/Info-RiLi/ent/RefEntw_Infoges_18_3_02.pdf

UrhGRegE 16.8.2002

Deutscher Bundestag (16.8.2002): Entwurf eines Gesetzes zur Regelung des Urheberrechts in der Informationsgesellschaft. Gesetzentwurf der Bundesregierung. BR-Drs. 684/02. Last visited: 20.8.2002. Available at: http://www.urheberrecht.org/topic/Info-RiLi/ent/RegE_UrhR_InfoG.pdf

UrhGRegE 6.11.2002

Deutscher Bundestag (6.11.2002): Entwurf eines Gesetzes zur Regelung des Urheberrechts in der Informationsgesellschaft. Gesetzentwurf der Bundesregierung. Drucksache 15/38. 15. Wahlperiode. Berlin. Elektronische Vorabfassung. Last visited: 7.11.2002. Available at: <http://dip.bundestag.de/btd/15/000/1500038.pdf>

UrhWahrnG

Gesetz über die Wahrnehmung von Urheberrechten und verwandten Schutzrechten (Urheberrechtswahrnehmungsgesetz) vom 9. September 1965. Zitiert nach: Hillig, Hans-Peter (2002): Urheber- und Verlagsrecht: Textausgabe. 9. neubearbeitete Ausgabe. Stand 1. Juli 2002. München. pp. 183–192.

URN (1997)

IETF RFC 2141 (May 1997): URN Syntax. Available at: <http://www.ietf.org/rfc/rfc2141.txt?number=2141>.

Urteil des Landgerichts Stuttgart (2001)

Urteil des Landgerichts Stuttgart vom 19. Juni 2001. 17 O 519/00. In: ZUM 7/2001. pp. 614-619.

Vahldiek (2000)

Vahldiek, Axel (14.7.2000): Bundesregierung will Urheberrechts-Abgaben für PC-Komponenten. Last visited: Available at: <http://www.heise.de/newsticker/data/axv-14.07.00-000/>

van Schyndel, Tirkel, Osborne (1994)

van Schyndel, R.G./ Tirkel, A.Z./ Osborne, C. F. (1994): A Digital Watermark. In: Proceedings of the international conference on image processing. Vol. 2. pp. 86–90. Austin. Texas, U.S.A.

Varian (1995)

Varian, Hal R. (1995): Pricing Information Goods Available at: <http://www.sims.berkeley.edu/~hal/Papers/price-info-goods.ps.Z>. Accessed: 06. 01. 2002.

Varian (1998)

Varian, Hal R. (1998): Markets for Information Goods. Prepared for Bank of Japan conference. June 18–19, 1998. Available at: <http://www.sims.berkeley.edu/~hal/Papers/japan/index.html>

Varian (2000)

Varian, Hal R. (December 2000): Buying, Sharing and Renting Information Goods. In: Journal of Industrial Economics. Vol. 48. pp. 473–488.

Varian (2001)

Varian, Hal R. (Dec. 16, 2001): Economics of Information Technology. Available at: <http://www.sims.berkeley.edu/~hal/Papers/multioli.pdf>.

Varian (2002)

Varian, Hal R. (2002): New Chips Can Keep a Tight Rein on Consumers. New York Times, July 4, 2002, at page C2.

Varian, Roehl (2001)

Varian, H./ Roehl, R. (May 2001): Circulating Libraries and Video Rental Stores. In: First Monday. 6(5). Available at: <http://firstmonday.org/>.

Vaughan–Nichols (2003)

Vaughan–Nichols, Steven J. (March 2003): How Trustworthy Is Trusted Computing? IEEE Computer 18.

VdS (2002)

VdS Bildungsmedien e.V. (21.8.2002): Stellungnahme zu §52 a des Regierungsentwurfes hinsichtlich eines Gesetzes zur Regelung des Urheberrechts in der Informationsgesellschaft. Frankfurt am Main.

VdS (2002a)

VdS Bildungsmedien e.V. (17.12.2002): Schulbuchverlage: Entwurf zum Urheberrechtsgesetz bedeutet Enteignung. Last visited: 17.12.2002. Available at: <http://www.vds-bildungsmedien.de/html/vds.htm>

VDZ (2002)

Verband Deutscher Zeitschriftenverleger (3.2002): Stellungnahme. In: CDU/CSU-Bundestagsfraktion (2002): pp. 82–87.

VDZ (2002a)

Verband Deutscher Zeitschriftenverleger (18.3.2002): Stellungnahme des Verbands Deutscher Zeitschriftenverleger zum Referentenentwurf für ein Gesetz zur Regelung zum Urheberrecht on der Informationsgesellschaft (Last visited 18. März 2002). Berlin. Last visited: 18.3.2002. Available at: http://www.vdz.de/mediabase/documents/Stellungnahme_VDZ.180302.pdf

verdi (2002)

ver.di — Vereinte Dienstleistungsgewerkschaft e. V. – Fachbereich Medien, Kunst und Industrie (2002j): über uns. Fachgruppe Musik. Last visited: 30.10.2002. Available at: http://www.verdi.de/0x0ad00f05_0x0000969b

verdi (2002a)

Industriegewerkschaft Medien (3.2002): Stellungnahme. In: CDU/CSU-Bundestagsfraktion (2002): pp. 64-69.

verdi (2002b)

ver.di – Vereinte Dienstleistungsgewerkschaft e. V. – Fachbereich Medien, Kunst und Industrie (19.4.2002): Referentenentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft. Brief von Wolfgang Schimmel (ver.di) an Dr. Irene Pakuscher (Bundesministerium der Justiz). Stuttgart.

VG Bild-Kunst Satzung

Verwertungsgesellschaft Bild-Kunst (8.7.2000): Satzung. Fassung vom 8. Juli 2000. Zitiert nach: Hillig, Hans-Peter (2002): Urheber- und Verlagsrecht: Textausgabe. 9. neubearbeitete Ausgabe. Stand 1. Juli 2002. München. pp. 240-248.

VG Bild-Kunst (2002)

Verwertungsgesellschaft Bild-Kunst (15.4.2002): STELLUNGNAHME der VG Bild-Kunst zum Referentenentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft. Bonn.

VG Wort Satzung

Verwertungsgesellschaft Wort (19.5.2001): Satzung. Fassung vom 19. Mai 2001. Zitiert nach: Hillig (2002): pp. 218-227.

VG Wort (2002)

Verwertungsgesellschaft Wort (3.2002): Stellungnahme. In: CDU/CSU-Bundestagsfraktion (2002): pp. 90-93.

Verlage und Wissenschaftler für ein faires Urheberrecht (2003)

Kampagnen-Website. Verantwortlich: Bösenverein es deutschen Buchhandels und Arbeitsgemeinschaft wissenschaftlicher Verleger c/o Mohr Siebeck Verlag. Abgerufen am 11.3.2003. Online in <http://www.52a.de>

Verlage und Wissenschaftler für ein faires Urheberrecht (2003a)

Geplante Urheberrechtsänderung gefährdet Fachverlage. Pressemitteilung vom 3.3.2003 Verantwortlich: Bösenverein es deutschen Buchhandels und Arbeitsgemeinschaft wissenschaftlicher Verleger c/o Mohr Siebeck Verlag. Abgerufen am 11.3.2003. Online in <http://www.52a.de>

Verlage und Wissenschaftler für ein faires Urheberrecht (2003b)

Geplante Urheberrechtsänderung. Stellungnahme zur Pressemeldung von Bundesjustizministerin Zypris. Pressemitteilung vom 6.3.2003 Verantwortlich: Bösenverein es deutschen Buchhandels und Arbeitsgemeinschaft wissenschaftlicher Verleger c/o Mohr Siebeck Verlag. Abgerufen am 11.3.2003. Online in <http://www.52a.de>

- Verlage und Wissenschaftler für ein faires Urheberrecht (2003d)
 Kampagne gegen Urheberrechtsänderung: Abgeordnete erhalten Notizbuch für „Ihr geistiges Eigentum“ . Pressemitteilung vom 25.3.2003 Verantwortlich: Bösenverein es deutschen Buchhandels und Arbeitsgemeinschaft wissenschaftlicher Verleger c/o Mohr Siebeck Verlag. Abgerufen am 15.4.2003. Online in <http://www.52a.de>
- Verlage und Wissenschaftler für ein faires Urheberrecht (2003e)
 Geplante Urheberrechtsänderung: Verleger protestierten vor der Staatsbibliothek in Berlin. Pressemitteilung vom 28.3.2003 Verantwortlich: Bösenverein es deutschen Buchhandels und Arbeitsgemeinschaft wissenschaftlicher Verleger c/o Mohr Siebeck Verlag. Abgerufen am 15.4.2003. Online in <http://www.52a.de>
- Vinje (1993)
 Vinje, Thomas C. (1993) in: Lehmann, Michael/ Tapper, Colin (ed.)(1993): A Handbook of European Software Law. pp. 89 et seq.
- Vinje (1996)
 Vinje, Thomas C. (1996): A brave new world of technical protection systems, will there still be room for copyright? In: E.I.P.R. No. 2. p. 431-440.
- Vinje (1996b)
 Vinje, Thomas C. (1996): Copyright Imperilled? In: EIPR 1996. p. 431.
- Vinje (1999)
 Vinje, Thomas (1999): Copyright Imperilled. E.I.P.R. 192, 193.
- V-ISAN
 Available at: <http://www.nlc-bnc.ca/iso/tc46sc9/20925.htm>
- VNU (2000)
 VNU Entertainment Marketing Solutions (2000): Measuring the Influence of Music File Sharing. New York.
- Vogel (1973)
 Vogel, Martin (1973): Der literarische Markt und die Entstehung des Verlags- und Urheberrechts bis zum Jahre 1800. In: GRUR.
- Vogel (1978)
 Vogel, Martin (1978): Deutsche Urheber- und Verlagsrechtsgeschichte zwischen 1450 und 1850. In: Archiv für Geschichte des Buchwesens 19.
- Vogel (1988)
 Vogel, Martin (1988): Grundzüge der Geschichte des Urheberrechts in Deutschland. In: Dittrich, Robert (ed.)(1988): Woher kommt das Urheberrecht und wohin geht es? Vienna. p. 119.
- Volokh (2003)
 Volokh, Eugene (2003): The Mechanisms of the Slippery Slope. In: 116 Harvard Law Review 1026.
- Voloshynovskiy, Pereira, Herrigel, Baumgartner, Pun (2000)
 Voloshynovskiy, Sviatoslav/ Pereira, Shelby/ Herrigel, Alexander/ Baumgartner, Nazanin/ Pun, Thierry (24–26 January 2000): Generalised watermarking attack based on watermark estimation and perceptual remodulation. In: Wong, Ping Wah/ Delp, Edward J. (eds.)(2000): Proceedings of SPIE conference on security and watermarking of multimedia contents II. Vol. 3971. San Jose, California. pp. 358–370.

VPRT (2001)

Verband Privater Rundfunk und Telekommunikation (19.11.2001): Diskussionsvorschlag des VPRT zur Umsetzung der Richtlinie 2001/29/EG zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft. Bonn.

VPRT (2002)

Verband Privater Rundfunk und Telekommunikation (3.2002): Stellungnahme. In: CDU/CSU-Bundestagsfraktion (2002): pp. 87-90.

VPRT (2002a)

Verband Privater Rundfunk und Telekommunikation (18.4.2002): Stellungnahme des VPRT zum Referentenentwurf des Bundesministeriums der Justiz für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft (18. März 2002). Last visited: 18.12.2002. Available at: <http://www.urheberrecht.org/topic/Info-RiLi/st/VPRTStellungRefE-2002-04-18.pdf>

VPRT (2002b)

Verband Privater Rundfunk und Telekommunikation (6.9.2002): Positionspapier des VPRT zum Regierungsentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft (version: 31. July 2002). Last visited: 18.12.2002. Available at: <http://www.urheberrecht.org/topic/Info-RiLi/st/PosRegEntwVPRT.pdf>

VZBV (2002)

Bundesverband der Verbraucherzentralen und Verbraucherverbände, Verbraucherzentrale Bundesverband (7.5.2002): Stellungnahme zum Referentenentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft (zu §53). Berlin.

VZBV (2002a)

Bundesverband der Verbraucherzentralen und Verbraucherverbände, Verbraucherzentrale Bundesverband (19.8.2002): Gesetzentwurf hebt Recht auf Privatkopien aus. Last visited: 19.8.2002. Available at: <http://www.vzbv.de>

— W —

Walker, Sharpe (2002)

Walker, Jacqui/ Sharpe, Andrew (2002): Digital Rights Management. In: 18 Computer Law & Security Report 259.

Wandtke (2002)

Wandtke, Artur (2002): Copyright und virtueller Markt in der Informationsgesellschaft. In: GRUR (2002). pp. 1-11.

Wandtke, Bullinger (2002)

Wandtke, Artur-Axel/ Bullinger, Winfried (2002): Praxiskommentar zum Urheberrecht. München.

Wang (2000)

Wang, C. (October 2000): A Security Architecture for Survivability Mechanisms. PhD Thesis. University of Virginia.

Ware (2002)

Ware, Donald R. (2002): Research Tool Patents: Judicial Remedies. 30 APILA Quarterly Journal 267.

Wargo (2001)

Wargo, S. (2001): Copyright and the Digital Medium. Available at: http://www.digitaltechnologyconsulting.com/pdf/Copyright_CEF.pdf. Accessed: 25.02.2002.

Warren, Brandeis (1890)

Warren, S./ Brandeis, L. (1890): The Right to Privacy. In: 4 Harvard Law Review. pp. 193–220.

Warschauer (2002)

Warschauer, Mark (7.2002): Reconceptualizing the Digital Divide. In: First Monday. Vol. 7. No. 7 (July 2002). Available at: http://firstmonday.org/issues/issue7_7/warschauer/index.html

Watts, Strogatz (1998)

Watts, D./ Strogatz, S. (1998): Collective dynamics of small world networks. Nature 393. pp. 440–442.

WCT

WIPO Copyright Treaty and Agreed statements Concerning the WIPO Copyright Treaty. Adopted in Geneva on December 20, 1996. The treaty can be found at [http://www.wipo.int/clea/docAxel Vahldieks/en/wo/wo033en.htm](http://www.wipo.int/clea/docAxel%20Vahldieks/en/wo/wo033en.htm)

WCT and WPPT (1996)

WIPO Copyright Treaty (WCT) and WIPO Performances and Phonograms Treaty (WPPT) of December 20, 1996.

Weber (1998)

Weber, R. (1998): Chablis – Market Analysis of Digital Payment Systems. Institut für Informatik, Technische Universität München. August 1998.

Weber (2003)

Weber, Damian (2003): Sicher unschädlich. Microsoft Palladium: Software–Aufsatz der Trusted Computing Platform. In: Linux Magazin. No. 4. pp. 68–73.

Weinberg (2002)

Weinberg, Jonathan (2002): Digital TV, Copy Control, and Public Policy. In: 20 Cardozo Arts & Entertainment Law Journal 277.

Weiser (2001a)

Weiser, Philip J. (2001): Networks Unplugged: Towards a Model of Compatibility Regulation Between Information Platforms. Available at <http://www.arxiv.org/html/cs/0109070>.

Weiser (2001b)

Weiser, Philip J. (2001): Internet Governance, Standard Setting, and Self-Regulation. 28 Northern Kentucky Law Review 822.

Weiser (2002)

Weiser, Philip J. (2002): Law and Information Platforms. In: 1 Journal on Telecommunications and High Technology Law 1.

de Werra (2001)

de Werra, J. (2001): What is a “technological measure” under the WIPO Treaties, the DMCA, the European Union Directives and other legislations (Japan, Australia). R.I.D.A. June 2001. p. 69.

Wersing (1973)

Wersing, Gerot (1973): Informationssoziologie. Hinweise zu einem informationswissenschaftlichen Teilbereich. Frankfurt.

whatis.com (2002)

whatis.com (2002): Definition: Digital Rights Management. Available at: <http://whatis.techtarget.com>. Keyword "Digital Rights Management".

Wheeler (1997)

Wheeler, D. (1997): Transactions using bets. In: Security Protocols, International Workshop 1996, Proceedings.

Wiebe (1997)

Wiebe, Andreas (1997): Information als Wirtschaftsgut. In: Fiedler, Herbert/Ullrich, Hanns (eds.) (1997): Information als Wirtschaftsgut. Köln.

Wigand (1988a)

Wigand, R.T. (1988): Communication network analysis: History and overview. In: Goldhaber, G.M./ Barnett, G.A. (eds.): Handbook of organizational communication. Norwood, NJ. pp. 319-359.

Wigand (1988b)

Wigand, R.T. (1988): Fünf Grundsätze für die erfolgreiche Einführung des Informations-Managements. In: Information Management. 3(2). pp. 24-30.

Wigand (1995a)

Wigand, R.T. (1995): Doing business on the Information Superhighway: Are we adding value? In: Business Journal. 9(24). pp. 3-15.

Wigand (1995b)

Wigand, R.T. (1995): Electronic commerce and reduced transaction costs: Firms' migration into highly interconnected electronic markets. In: Electronic Markets. 16/17. pp. 1-5.

Wigand (1996)

Wigand, R.T. (1996): An overview of electronic commerce and markets. Paper presented to the Annual Conference of the International Communication Association. Chicago. May 23-27.

Wigand (1997a)

Wigand, R.T. (1997): Electronic data interchange: A transaction cost perspective. EDI Forum. 10(1). pp. 60.

Wigand (1997b)

Wigand, R.T. (1997): Electronic commerce. The Information Society. 13. pp. 1-16.

Wigand (2000)

Wigand, R.T. (2000): Old Media Beats New Technology—For Now. In: Policy Forum, ICA Newsletter. December. p. 5.

Wigand, Frankwick (1989)

Wigand, R.T./ Frankwick, G.L. (1989): Interorganizational communication and technology transfer: Industry-government-university linkages. In: International Journal of Technology Management. 4(1). pp. 63-76.

Wigand, Picot, Reichwald (1997)

Wigand, R.T./ Picot, A./ Reichwald, R. (1997): Information, organization and management: Expanding markets and corporate boundaries. Chichester, England.

Wilkens (2003)

Wilkens, Andreas (5.2.2003): HP wettert gegen Urheber-Pauschale für PCs. Abgerufen am 12.4.2003. Online in: <http://www.heise.de/newsticker/data/anw-05.02.03-007/>

- Wilkens, Zota (2002)
 Wilkens, Andreas / Zota, Volker (2002): Streitpauschale. Branchenverband und Verwerter brechen Gespräche ab. In: c't 2002. Heft 6.
- Williamson (1975)
 Williamson, O.E. (1975): Markets and hierarchies: Analysis and antitrust implications. A study in the economics of internal organization. New York.
- Williamson (1981a)
 Williamson, O.E. (1981): The modern corporation: Origin, evolution attributes. In: Journal of Economic Literature. 19. pp. 1537–1568.
- Williamson (1981b)
 Williamson, O.E. (1981): The economics of organization: The transaction cost approach. In: American Journal of Sociology. 87(3). pp. 548–577.
- Williamson (1985)
 Williamson, O.E. (1985): The Economic Institutions of Capitalism: Firms, Markets, Relational Contracting. New York.
- Williamson (1986)
 Williamson, O.E. (1986). The economic institutions of capitalism: Firms, markets, relational contracting. 11th Ed. New York.
- Winghardt (2002)
 Winghardt, Stefan (2002): Kopiervergütung für den PC. ZUM 5/2002. pp. 349–361. p. 349.
- Wintermute (2003)
 Wintermute (Jan. 25, 2003): TCPA and Palladium Technical Analysis. Version 1.06. Available at: <http://wintermute.homelinux.org/miscelanea/TCPA%20Security.txt>.
- WM9–DRM
 Windows Media 9 Series — Digital Rights Management. Available at: <http://www.microsoft.com/windows/windowsmedia/drm.aspx>.
- Wobst (2001)
 Wobst, Bernhard (2001): Abenteuer Kryptologie. Addison–Wesley. 3. ed.
- Wold, Blum, Keislar, Wheaton (1996)
 Wold, E./ Blum, T./ Keislar, D./ Wheaton, J. (1996): “Content–based classification, search and retrieval of audio”. IEEE Multimedia 3(3):27–36.
- WPPT
 WIPO Performances and Phonograms Treaty and Agreed Statements Concerning the WIPO Performances and Phonograms Treaty. Adopted in Geneva on December 20, 1996. The treaty can be found at <http://www.wipo.int/clea/docs/en/wo/wo034en.htm>
- Wright, Cowan, Smalley, Morris, Kroah–Hartman (2002)
 Wright, Chris/ Cowan, Crispin/ Smalley, Stephen/ Morris, James/ Kroah–Hartman, Greg (2002): Linux Security Modules: General Security Support for the Linux Kernel. In: Ottawa Linux Symposium 2002. Proceedings. Available at: <http://www.cse.ogi.edu/~crispin/>. Last visited: 09 March 2003.
- WSJE (2002)
 WSJE (2002): Recording Industry is Online - Minus Music and Listeners. Wall Street Journal Europe. 7.5.2002.

W3C (1999)

W3C (1999): Namespaces in XML — 14 January 1999. Available at: <http://www.w3.org/TR/REC-xml-names/>.

W3C (2001)

W3C (Oct 2001): Uniform Resource Identifier (URI) Activity Statement. Available at: <http://www.w3.org/Addressing/Activity>.

W3C (2002)

W3C (Sept 2002): Open Digital Rights Language (ODRL) Version 1.1. Available at: <http://www.w3.org/TR/odrl/>.

— X —

X.509 (1989)

Recommendation X.509. The Directory–Authentication Framework. Consultation Committee. International Telephone and Telegraph. International Telecommunications Union. Geneva.

— Y —

Yacobi (1997)

Yacobi, Y. (1997): On the continuum between on–line and off–line e–cash systems. In: Financial Cryptography, First International Conference (FC '97), Proceedings.

Yang, Weimann, Mitropoulos (2002)

Yang, Chun–Lei/ Weimann, Joachim/ Mitropoulos, Atanasios (2002): Effects of Bargaining Power in Sequential Bargaining Games: An Experiment.

Yasukawa (2002)

Yasukawa, Michiko (2002): A Method for Making Dynamic License Agreements in Reuse of Web Contents. 43 (SIG 2) IPSJ Transactions on Databases 179 (in Japanese).

Yasukawa (2003)

Yasukawa, Michiko (2003): A Dynamic License Agreement System for Reuse of Web Contents. In: Meersman, Robert/ Aberer, Karl/ Dillon, Tharam S. (eds.) (2003): Semantic Issues in E–Commerce Systems. IFIP TC2/WG2.6 Ninth Working Conference on Database Semantics. Boston. p. 35.

Yodaiken (2002)

Yodaiken, Victor (2002): Digital Rights Management Issues for Real–Time and Safety/Mission Critical Software. In: FSMLabs White Paper. Available at: http://www.fsmlabs.com/developers/white_ppapers/drm.pdf. Last visited: 26 March 2003.

Yoon (2001)

Yoon, K. (2001): The Optimal Level of Copyright Protection. Department of Economics. Korea University. Seoul.

Yung (2000)

Yung, Moti (2000): Payment systems: The next generation. In: Financial Cryptography, 4th International Conference (FC 2000), Proceedings.

— Z —

Zecher (2002)

Zecher, Jan (6.2002): Die Umsetzung der EU-Urheberrechtsrichtlinie in deutsches Recht II. Diskussionsbericht von der gleich lautenden Arbeitssitzung des Instituts für Urheber- und Medienrecht am 22. März 2002. In: ZUM. 6.2002. 451-457.

Zerdick, Picot, Schrape, et. al. (2000)

Zerdick, Axel/ Picot, Arnold/ Schrape, Klaus/ Artopé, Alexander/ Goldhammer, Klaus/ Lange, Ulrich T./ Vierkant, Eckart/ López-Escobar, Esteban/ Silverstone, Roger (2000): E-conomics: strategies for the digital marketplace. Berlin.

Zerdick et al. (1999)

Zerdick, A. et al. (1999): Die Internet-Ökonomie — Strategien für die digitale Wirtschaft. Berlin, Heidelberg.

Zhao, Koch (1995)

Zhao, J./ Koch, E. (August 1995): Embedding robust labels into images for copyright protection. In: Proceedings of the international congress on intellectual property rights for specialised information, knowledge and new Technologies. Vienna. Austria.

Zittrain (2000)

Zittrain, Jonathan (2000): What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication. In: 52 Stanford Law Review. pp. 1201–1250.

Zombik (1998)

Zombik, Peter (9.6.1998): Music-on-Demand: „Tanz auf dem Vulkan“ oder „Gib dem Affen Zucker“? Chancen und Gefahren der neuen Technologien. Last visited: 24.4.2002. Available at: <http://www.ifpi.de/recht/re-6.htm>

ZPÜ Gesellschaftsvertrag

Zentralstelle für private überspielungsrechte (21.12.1992): Gesellschaftsvertrag. Fassung vom 21.12.1992. Zitiert nach: Hillig (2002): pp. 288-290.

ZPÜ Inkassovertrag

Zentralstelle für private überspielungsrechte (10.5.1989): Inkassovertrag. Fassung vom 21.12.1992. Zitiert nach: Hillig (2002): pp. 289-290.

ZVEI (7.9.2000)

Position des ZVEI zu den Vorstellungen der Bundesjustizministerin zur künftigen Urheberrechtspolitik. Last visited: 7.9.2000. Available at: <http://www.gfu.de/Pages/newshe/urheber.htm>

D Index

A

Access Right 574
ACM's Copyright Policy 404
Acquis Communautaire 407, 415
Added Value 6
ADo²Ra 160
Adobe PDF 207
Advanced DRM Systems 358
Advanced PDF Password
 Recovery 217
AES 69
AHRA 367
Algorithm
 Asymmetric 63
 Cryptographic 63, 69
 Restricted 63
 Secure Hash 73
 Symmetric 63
Analog Hole 227
Anonymity 435
Anti-Circumvention 293, 609
 Regulation 462, 509, 544, 559, 612
 Scientific Research 612
Anticounterfeiting Amendments 394
Asymmetric Algorithm 63, 69
Attack
 Brute-Force 218
 on Arbitrary DRM Systems 213
 on Microsoft's Audio
 DRM Systems 207
 on Video DRM Systems 216
Audio Fingerprinting 96
Audio Home Recording Act 367, 614
Authentication 8, 70

Mechanisms 164, 168
Protocols 75
Authorization 152, 157

B

Bandwidth 282
Beale Screamer 210, 529
Benefits of DRM 17
Berne Convention 406
BIEM 450
Billing Systems 279
Bits of Power 396
Blind Signature 126
BOBE 359
Booking 151, 156
BPDG 631, 651
Broadcast Protection 631, 651
Business Models 271, 272, 298

C

CBDTPA 376, 390, 651
CDRL 107
Celestial Jukebox 283
Certification
 Authority 73, 184
 Certificate 9
CGMS 632
Circumvention of Copyright
 Protection Systems 13, 369, 509,
 559
CISAC 450
Clearing 152
Coase Theorem 288
Code is Law 580
Collecting Societies 450

- Commercial DRM Products 159
 - Competing with Piracy 231
 - Competition in the
 - Platform Market 619
 - Concerns against the DMCA 372
 - Conditional Access
 - Directive 575
 - System 357, 622
 - Consequences for Teaching
 - and Research 520
 - Consumer Acceptance for
 - Protection Technologies 315
 - Consumer Broadband and Digital
 - Television Promotion Act 390, 651
 - Consumer Needs 309
 - Consumer Willingness to Pay 310
 - Content
 - Aggregation 281
 - Based Identification 93
 - Consumption 152, 157
 - Description 7
 - Distribution 151, 156
 - for Free 321
 - Identification 7
 - Preparation 151, 156
 - Protection
 - for Recordable Media 631
 - Provision 151, 155
 - Rights Server 159
 - Safekeeping 151, 155
 - Scrambling System (CSS)
 - 9, 13, 175, 502, 632
 - ContentGuard 106
 - Copy Generation Management
 - System 632
 - Copy Protection
 - and DRM under the EU Directive 507
 - Legal Aspects 502
 - Technical Working Group 360, 631
 - Copyright
 - Box 191
 - Economic Role 236
 - Enforcement 4
 - Exception/Exemption
 - 447, 453, 492, 495, 536, 538, 544, 601, 607, 611
 - Education and Research 520, 540
 - Enforcement 544
 - Remuneration Systems 546
 - Legislation in the
 - European Union 406
 - Management
 - at Universities 525
 - Information 371
 - Core Root of Trust
 - for Measurement 184
 - Corporate DRM 14
 - Cost 14, 15
 - Copy Protection 274
 - Theory
 - Transaction 258
 - CPRM 631
 - CPTWG 360, 631
 - Creative Commons 107, 605
 - CRIM 184
 - Crucial Elements of DRM 5
 - Cryptographic Algorithm 63
 - CSS 9, 13, 175, 502, 632
 - Custom Digital
 - Rights Language 107
 - CyberCash 124
- D**
- D-Space Project 46
 - Darknet 224, 303, 344
 - Data Encryption Standard 64
 - Data Integrity Register 183
 - Database
 - Treaty and Legislation 395
 - Deadweight Loss of a Monopoly 237
 - DeCSS 9, 13, 359, 399, 579
 - DES 64
 - Devices 282
 - Digital Black Market 282
 - Digital Copies
 - under the EU Directive 458
 - under the German Copyright Act 458
 - Digital Management of Rights 4
 - Digital Millennium Copyright Act
 - 293, 296, 352, 368, 388, 466, 612
 - Digital Object Identifiers 8
 - Digital Property
 - Rights Language 107
 - Digital Restrictions Management 192
 - Digital Rights
 - Expression Language 107
 - Digital Transmission Content
 - Protection 632
 - Digital Video Broadcasting Project 622

- Digital World Services 160
 - Directive on Electronic Commerce 413
 - Directive on the Artists'
 - Resale Right 407
 - Disintermediation 254
 - DivX 324, 359
 - DMCA 293, 296, 352, 368, 388, 466, 612
 - Concerns against 372
 - DOI 8
 - DPRL 107
 - DREL 107
 - DRM
 - and Competition 619
 - and Privacy 617
 - and Research 612
 - and Standardization 630
 - Benefits 17
 - Commercial Products 159
 - Components
 - Patenting 621
 - Crucial Elements 5
 - Definition 3, 4
 - Dynamic 602
 - Economic Aspects 5
 - Evaluation Criteria 10
 - External factors 5
 - in Laser Printers 623
 - International Aspects 6
 - Internet 139
 - Maintenance 23
 - Mobile 138
 - Protection 508
 - Security 21
 - Social Aspects 5
 - Standardization 162
 - Technology 4
 - Competition 622
 - License Agreements 609, 622
 - DRM Systems
 - Attacks 207
 - Audio 213
 - Video 216
 - Coast 14
 - Dynamic 602
 - Evaluation Criteria 10
 - Functionalities 150
 - Leakage 11
 - Microsoft 329
 - Problem of Uptate 14
 - Requirements 16
 - Sample 154
 - Security 11
 - Variant 159
 - droit d'auteur 609
 - DTCP 632
 - Dublin Core Metadata
 - Initiative 54, 93, 605
 - DVB Content Protection
 - and Copy Management 632
 - DVD
 - CCA v. Bunner 401
 - related Cases 398
- E**
- eBook 112, 170, 217, 219
 - EBU 93
 - Economic Aspects of DRM 5
 - Economic Role of Copyright 236
 - Economic Theory of
 - unauthorized Copying 239
 - ElcomSoft 217, 402
 - Eldred v. Ashcroft 397
 - Electronic
 - Brokerage Effect 254
 - Cash 10
 - Integration Effect 254
 - Markets 251
 - Media Management System 112, 160
 - Payment System 113
 - Strategic Networking Effect 254
 - EMMS 112, 160
 - Encryption Research 370
 - Equitable Remuneration 513
 - Ergonomy 15
 - Evaluation Criteria
 - for DRM Systems 10
 - Event Report 9
 - Extensibility 12
 - eXtensible Media
 - Commerce Language 107
 - Extent of Limitations 522
- F**
- Fair Compensation 508, 513
 - under the EU Directive 454
 - Fair Use 6, 170, 372, 472, 599, 608, 609
 - Default Settings 608
 - Felten 401, 612
 - Financial Services
 - Technology Consortium 123

Fingerprinting 9, 93, 96, 362
 First Amendment 373
 Flexibility 12
 Forensic technologies 9
 4C 631
 Framework
 <indec> 52
 Trust 171
 Fraunhofer IIS 7
 Free Movement of Goods 628
 Free Riding 277, 351, 355
 Freedom of Speech 373
 FreeMe 210
 Freenet 351, 354
 FTSC 123
 Fuzzy Hashing 229

G

German Copyright
 Act of 1965 483
 Amendment Act of 2003 491
 GNU General Public License 201, 606
 Gnutella 350, 355
 Green Paper on Copyright and
 the Challenge of Technology 407

H

Handle System 45
 HDCP 632, 652
 HDTV 169
 Hollings Bill 375
 Hybrid Systems 70

I

iKey Protocol 124
 Identification 70
 Identifiers 28
 of People 8
 Unique 29
 IFRRO 450
 Impaction Creativity and Innovation 599
 Implementability 12
 Importance of Credibility 274
 Imprimatur 8
 <indec>
 Framework 52
 2rdd Project 106
 Indirect Appropriability 243, 249
 InfoSoc Directive 576
 Integration 15

Intellectual Property Rights
 Working Group 366
 Intermediation Theory 260
 International Aspects of DRM 6
 International Standard
 Audio-visual Numbers 8
 Book Number 7, 30
 Recording Codes 7
 Work Code 7

Internet
 based Innovation 288
 DRM 139
 Piracy 302
 Interoperability 13, 15, 20, 140
 Interpreter
 REL 108
 InterTrust 7, 159
 IPMP 169, 171, 176
 ISAN 8
 ISBN 7, 30
 ISO 7, 13
 ISO 11179 55
 ISO Authentication Framework 73
 ISO/MPEG's Right
 Expression Language 7
 ISRC 7
 ISWC 7

J

Johansen, Jon 399

K

KaZaA 321, 328, 355
 Kerberos 123
 Kerckhoff Principle 613
 Key Space 63

L

Lack of Anonymity 351
 LaGrande 22, 200
 Leakage of DRM Systems 11, 345
 Legal Protection of TPM 22
 Levies 282, 447, 546, 604
 Collection 451
 Compensation 523
 in the Digital Age 457
 Legal Framework 453
 Lump-Sum 493
 Reprographic Private Uses 451
 under the EU Directive 454

Lexmark Printers 625
 Liability Rules 614
 License Phrasing 151, 155
 Component 108
 Licensing 14
 Linux 605

M

Maintenance of DRM 23
 Making Available Right 492, 495, 582
 Managing Digital Rights 4
 Marketing 261
 Mediation 254
 Message Authentication Techniques 72
 Metadata 4, 26
 Dublin Core Initiative 54, 605
 System 618
 Well-formed 52
 Mickey Mouse Extension Act 386
 Microsoft 7, 207, 208, 210
 DRM 329
 eBook Reader 219
 License Server 159
 Media Player 207, 321
 Palladium 22, 198, 222, 632, 638
 MilliCent 131
 MMP 7
 Mnemosyne 354
 Mobile DRM 138
 Mobile Music 271
 Revenue Sources 281
 Scenario Matrix 282
 Scenarios 279
 Mobility 16
 Monopoly
 Deadweight Loss 237
 MPEG 7, 13, 632
 MPEG-7 97
 MPEG-21 59, 106, 167, 176
 Multimedia Protection Protocol 7
 Music Service Provider 283
 MusicNet 112, 327

N

Napster 350
 National Infrastructure 366
 NetBill 123
 NetCheque 123
 Next-Generation Secure
 Computing Base 198, 222, 638

Nexus 199, 639
 No Rivalry in Consumption 274
 Notice & Take Down 413

O

OASIS 106, 167, 631
 Obfuscation techniques 10
 ODRL 103, 105, 167
 Example 109
 Offer Creation 151, 155
 OMA 105, 141, 176, 278
 DRM 340
 Rights Expression Language 146
 Ontology 28
 Open Digital
 Rights Language 103, 105
 Open eBook Forum 106
 Open Mobile Alliance 105, 141, 176, 278
 DRM 340
 Open Source 294
 TCPA 200
 Open Standards 335
 Open Technology Standardization 336
 OpenCable specification 632
 OpenEBook 167
 Openness 12
 OPIMA 169

P

Palladium 22, 198, 222, 632, 638
 Patenting DRM Components 621
 Pay-per-Use 604
 Paybox 136
 Payment 152, 156
 Payment systems 10
 PDF
 Adobe 207
 Advanced Password Recovery 217
 Peer-to-Peer
 Distribution 282
 Networks 327, 349, 356
 Piracy Prevention Act 392
 Persistent Uniform
 Resource Locator 50
 Persistent URL 50
 PII 42
 Piracy 224, 277
 Competing 231
 Internet 302
 PKI 153

Platform Configuration Register 183
 popfile.de 328
 PressPlay 112, 327
 Privacy 8, 10, 23, 418, 558
 Enhancing Technologies 436
 Implication 618
 Personal 371
 Private Copying 447, 537, 614
 Exception/Exemption 538
 EU 507
 Germany 504
 under the NGCA 512
 Private Goods 277
 Private Use 493
 Problem of updates
 of DRM Systems 14
 Promotion 281
 Proprietary Mechanisms 153
 Protection of DRM 508
 Provider
 Music Service 283
 Public Key
 Certificates 73
 Infrastructure 153
 Publisher Item Identifier 42
 PURL 50

R

RDD 19, 60
 RDF 55, 605
 Real Player 207
 Recording Industry Association
 of America 423, 612
 Reference Monitor 188
 Reference Validation Mechanism 189
 Region Coding 628
 Reintermediation 254
 REL 19, 59, 101, 603
 Interpreter 108
 OMA 146
 Remote Attestation 195
 Remuneration Systems 546
 Requirements for DRM Systems 16
 Resource Description Framework 55, 605
 Restricted Algorithm 63
 Reverse Engineering 370
 DRM-Protected Platforms 620
 RIAA 401, 423, 612
 Rights Data Dictionary 7, 19, 60, 104
 Rights Expression 7

 Language 19, 59, 101, 603
 Mechanism 164, 167
 Rights Grammar 107
 Rights Language Concept 103
 Rights Locker 161, 600
 Rights Management Information 443
 Legal Aspects 496
 Rijndael 7, 69
 RSA 70
 RVM 189

S

Sample DRM System 154
 SCMS 367, 651
 SDK 6 207
 SDMI 278, 330, 360, 612, 631
 Phase I watermark 9
 Secure Container 7, 62, 78, 151
 Methods 226
 Secure Electronic Transaction 125
 Secure Hash Algorithm 73
 Secure Player 164, 168
 Secure Socket Layer 76, 124
 Secure Storage 166
 Security 15
 of DRM 21
 of DRM Systems 11
 of IT 179
 Security Aspects of
 Client DRM Systems 79
 Security Systems Standards and
 Certification Act 375
 Security Testing 371
 Serial Copy Management
 System 367, 467, 651
 Serial Item and
 Contribution Identifier 43
 SET 125
 SHA 73
 SICI 43
 Sklyarov, Dmitry 217, 402
 Small Worlds Networks 347, 356
 SMPTE 7, 93
 Sneaker Net 347, 348
 Social Aspects of DRM 5
 Software Protection Directive 575
 Sony Aibo Dog 623
 Space Shifting 601
 Specification 93
 Sponsorship 281

- SSC 625
 - SSL 76, 124
 - Standardization 162, 334
 - Functions 336
 - Open Technology 336
 - Static Control Components 625
 - Strategic Networking 263
 - Subscription 281
 - Models 284
 - Superdistribution 140, 285
 - Symmetric Algorithm 63
 - Symmetric Rights Expression
 - Languages 607
- T**
- Tamper Resistance 10
 - Taxation 282
 - TCPA 10, 22, 178, 222, 632, 633
 - Evaluation Criteria 188
 - LaGrande 200
 - Microsoft Palladium
 - 22, 198, 222, 632, 638
 - Module 183
 - Open Source 200
 - Support Service 184
 - TSS 184
 - TCSEC 188
 - TEACH Act 521, 525
 - Technical Protection Measures
 - Legal Aspects 496
 - Technology, Education, and Copyright
 - Harmonization Act 521, 525
 - Three Legged Stool of DRM 5
 - Three Steps Test 459
 - TLS 124
 - Token 152
 - TopicMaps Specification 55
 - TPM 183
 - Legal Protection 22
 - Trade Secrets 579
 - Transaction Cost Theory 258
 - Transport Layer Security 124
 - Trust 9, 11, 15
 - Framework 171
 - Trusted Party 9
 - Trusted System 191
- U**
- Unauthorized
 - Acquisition 225
 - Use 225
 - Unfair Competition 579
 - Unfuck 208
 - Uniform Resource
 - Identifier 48
 - Name 48
 - Unique Identification 29
 - Universities
 - Copyright Management 525
 - URI 48
 - URN 48
 - Use Contracts 544
 - Usenet 350
 - User Authentication Techniques 71
 - User Friendliness 10, 15
 - User Identification 8
 - User Rights 386
- V**
- Value Chain 3, 8
 - Verizon 423
 - Violation of the First
 - Amendment by the DMCA 373
 - Vulnerabilities 226
- W**
- Watermarking 9, 81, 227, 360, 362
 - Algorithm 81
 - Detectors 362
 - WCT 406, 574
 - Well-formed Metadata 52
 - Windows Media
 - Player 207, 321, 329
 - Rights Manager 112, 159
 - SDK 6 207
 - WIPO
 - Copyright Treaty 368, 406, 574
 - Performance Treaty 368, 406, 574
 - Phonogram Treaty 368, 406, 574
 - Treaties 466
 - Workflow Control 152
 - Working Group on Intellectual
 - Property Rights 366
- X**
- X.509 Protocol 73, 168
 - XMCL 107
 - XML 35, 55, 102, 167, 631
 - XrML 60, 106, 167, 603, 608
 - Example 110