MPI Studies on Intellectual Property and Competition Law 28

Mor Bakhoum · Beatriz Conde Gallego
Mark-Oliver Mackenrodt
Gintarė Surblytė-Namavičienė *Editors*

Personal Data in Competition, Consumer Protection and Intellectual Property Law

Towards a Holistic Approach?

Springer

Max Planck Institute for
Innovation and Competition

MAX-PLANCK-GESELLSCHAFT

More information about this series at
http://www.springer.com/series/7760

MPI Studies on Intellectual Property and Competition Law

Volume 28

Edited by

Josef Drexl
Reto M. Hilty
Joseph Straus

Mor Bakhoum • Beatriz Conde Gallego •
Mark-Oliver Mackenrodt •
Gintarė Surblytė-Namavičienė
Editors

Personal Data in Competition, Consumer Protection and Intellectual Property Law

Towards a Holistic Approach?

Springer

Editors
Mor Bakhoum
Max Planck Institute for Innovation and Competition
Munich, Germany

Beatriz Conde Gallego
Max Planck Institute for Innovation and Competition
Munich, Germany

Mark-Oliver Mackenrodt
Max Planck Institute for Innovation and Competition
Munich, Germany

Gintarė Surblytė-Namavičienė
Faculty of Law
Vilnius University
Vilnius, Lithuania

ISSN 2191-5822 ISSN 2191-5830 (electronic)
MPI Studies on Intellectual Property and Competition Law
ISBN 978-3-662-57645-8 ISBN 978-3-662-57646-5 (eBook)
https://doi.org/10.1007/978-3-662-57646-5

Library of Congress Control Number: 2018955625

This Springer imprint is published by the registered company Springer-Verlag GmbH, DE part of Springer Nature.
The registered company address is: Heidelberger Platz 3, 14197 Berlin, Germany

Contents

Introducing a Holistic Approach to Personal Data 1
Mor Bakhoum, Beatriz Conde Gallego, Mark-Oliver Mackenrodt, and Gintarė Surblytė-Namavičienė

Part I Fundamentals of Personal Data: Between Personal Property Rights and Regulation

The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right? 7
Manon Oostveen and Kristina Irion

From Personality to Property? 27
Andreas Sattler

The Failure of Control Rights in the Big Data Era: Does a Holistic Approach Offer a Solution? 55
Helena Ursic

The Ambivalence of Algorithms 85
Philipp Hacker

Part II Personal Data and Competition Law

Blurring Boundaries of Consumer Welfare 121
Inge Graef

The Rise of Big Data and the Loss of Privacy 153
Anca D. Chirita

Big Data, Open Data, Privacy Regulations, Intellectual Property and Competition Law in an Internet-of-Things World: The Issue of Accessing Data 191
Björn Lundqvist

A Competition-Law-Oriented Look at the Application of Data Protection and IP Law to the Internet of Things: Towards a Wider 'Holistic Approach' 215
Jacopo Ciani

Part III Personal Data, Civil Law and Consumer Protection

Proprietary Rights in Digital Data? Normative Perspectives and Principles of Civil Law 253
Lennart Chrobak

Personal Data After the Death of the Data Subject—Exploring Possible Features of a Holistic Approach 273
Mark-Oliver Mackenrodt

The General Data Protection Regulation and Civil Liability 303
Emmanuela Truli

Protecting Children Online: Combining the Rationale and Rules of Personal Data Protection Law and Consumer Protection Law 331
Milda Mačėnaitė

Personal-Data and Consumer Protection: What Do They Have in Common? 377
Matilde Ratti

Part IV Personal Data, IP, Unfair Competition and Regulation

The Right to Data Portability and Cloud Computing Consumer Laws . . . 397
Davide Mula

The Interface Between Data Protection and IP Law: The Case of Trade Secrets and the Database *sui generis* Right in Marketing Operations, and the Ownership of Raw Data in Big Data Analysis 411
Francesco Banterle

Data as Digital Assets. The Case of Targeted Advertising 445
Guido Noto La Diega

Binding Corporate Rules As a New Concept for Data Protection in Data Transfers 501
Bianka Maksó

The Power Paradigm in Private Law 527
Heiko Richter

Introducing a Holistic Approach to Personal Data

Mor Bakhoum, Beatriz Conde Gallego, Mark-Oliver Mackenrodt, and Gintarė Surblytė-Namavičienė

Personal data and their use constitute a fundamental building block of the digital economy. An increasing number of business models rely on personal data as a key input. In exchange for sharing their data, users benefit from personalized and innovative services. At the same time, firms' collection, processing and use of personal data pose questions about privacy and fundamental rights. Moreover, given the great commercial and strategic value of personal data, their accumulation, control and use may raise competition concerns and negatively affect consumers. It is, thus, a challenging task to develop a legal framework that ensures an adequate level of protection of personal data while at the same time providing an open and level playing field for businesses to develop innovative data-based services.

Beyond being subject to the application of the data protection rules, the handling of personal data can be affected and, thereby, be directly and indirectly regulated by different fields of law like competition law, unfair competition law, consumer protection

Dr. Mor Bakhoum, LL.M. (Chicago-Kent), LL.M. (Lausanne), is an Affiliated Research Fellow, Max Planck Institute for Innovation and Competition, Munich.
Dr. Beatriz Conde Gallego, LL.M. (Würzburg), is a Senior Researcher, Max Planck Institute for Innovation and Competition, Munich.
Dr. Dr. Mark-Oliver Mackenrodt, LL.M. (NYU), Attorney at Law (New York), is a Senior Researcher at the Max Planck Institute for Innovation and Competition, Munich.
Dr. Gintarė Surblytė-Namavičienė, LL.M. (München), Lecturer, Vilnius University, Faculty of Law, Lithuania. She was a Senior Research Fellow at the Max Planck Institute for Innovation and Competition in Munich from June 2011 till June 2017.

M. Bakhoum · B. C. Gallego · M.-O. Mackenrodt (✉)
Max Planck Institute for Innovation and Competition, Munich, Germany
e-mail: mark-oliver.mackenrodt@ip.mpg.de

G. Surblytė-Namavičienė
Faculty of Law, Vilnius University, Vilnius, Lithuania

M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law*, MPI Studies on Intellectual Property and Competition Law 28, https://doi.org/10.1007/978-3-662-57646-5_1

law and IP law. To what degree and why are different fields of law particularly blind or sensitive to personal data? Are there conflicts between the objectives of the different legal areas and data protection? How can the specific approach of one area of law to personal data inspire or complement other fields of law? How can a holistic legal approach to personal data be developed? Under the guidance of these overarching questions, the contributions of this book examine the significance and legal treatment of personal data in different areas of law, seeking to identify shortcomings and common principles and exploring ways to develop an integrated legal approach to personal data.

Starting with the fundamentals of personal data, Manon Oostveen and Kristina Irion (University of Amsterdam) highlight the constitutional dimension of the protection of personal data and the character of the data protection right as an enabling right for other fundamental rights such as the right to privacy. Approached as an enabling right, EU data protection law protects against short- and long-term effects of the kinds of processing of personal data that are prevalent today. The constitutional underpinnings of the protection of personal data should be perceived as going beyond what is expressly codified in the European General Data Protection Regulation (EU GDPR). In this regard, the authors argue that alternative legal approaches for the protection of individual rights and freedoms should be explored. Helena Ursic (Leiden University) shows how the EU GDPR already reflects concepts from other legal fields such as the data subjects' rights to data portability, the right to be forgotten and the right to information. This approach of the EU GDPR shows the potential to build at the EU level a holistic approach in relation to the protection of personal data which takes into account the required balance between data subjects' rights and the need to build a data-driven economy. In complement to the idea of a more integrated regulatory approach, Andreas Sattler (Ludwig Maximilians University, Munich) argues for an empowerment of data subjects by introducing "a right to one's data". This would result in a right of dual character as it would be property-like while integrating strong aspects of a personality right. Philipp Hacker (European University Institute, Florence) discusses the legitimacy and pitfalls of a regulatory approach where the legislature analyses the individual citizen's behaviour by using algorithms in order to create a personalized law. While personalized law may mitigate "digital market failures" resulting from the use of behavioural algorithms, it also raises legitimacy issues.

Focusing on competition law and personal data, Inge Graef (KU Leuven) stresses the complementarity of competition, consumer protection and data protection in as far as these fields of law promote different aspects of consumer welfare. In line with the investigation of the German Bundeskartellamt in its Facebook case she favours the use of data protection and consumer law principles as benchmarks for analysing whether an abuse of dominance under competition rules exists. Anca Chirita (Durham University) provides a detailed examination of the privacy policies of some of the most relevant online platforms and argues in favour of a competition law intervention to tackle price discrimination based on data misuse as a particular form of abuse of dominance. Moreover, while still immersed in the effort to create a coherent legal framework for the digital economy, policy makers and enforcers are

facing new challenges arising from rapid and novel technological developments. With the advance of the Internet of Things (IoT), sensor-enabled devices increasingly collect data—many of them personal—about their environment. Privacy concerns that are already present today will be amplified in the IoT scenario of the future, which will test the adequacy of the traditional "notice and consent" data protection model. Likewise, new data-related IoT business models are deeply changing the dynamics of competition. Jacopo Ciani (University of Milan) and Björn Lundqvist (Copenhagen Business School) in their contributions elaborate on the manifold and complex legal issues raised by the emerging IoT.

Lennart Chrobak (University of Zurich) opens his study by classifying data and information and by discussing data as an economic input factor and as a legal input factor. He then analyses how personal data are approached by the existing civil law rules and finds substantial differences between the different fields of civil law. For example, the applicability of property law to personal data is determined to be very limited due to the quite strict interpretation of the fundamental property law principles of *numerus clausus*, specificity and publicity. By contrast, he finds the law of obligations widely applicable to personal data cases, as many imbalances between the rights and the duties of the contracting parties can be found. In conclusion, Chrobak points to recent legal and technological approaches which seek to diminish deficiencies in the treatment of data as a new kind of legal object. Mark-Oliver Mackenrodt (Max Planck Institute for Innovation and Competition, Munich) examines the legal treatment of personal data after the death of the data subject by different fields of law, including inheritance law, contract law, intellectual property law, privacy law, the right to personality and telecommunications law, in order to explore and identify possible features of a holistic approach to personal data. Emmanuela Truli (Athens University for Economics and Business) examines the conditions under which a plaintiff who has suffered harm from a breach of the data protection rules can sue for private law damages according to the new EU GDPR. In comparison with the old Data Protection Directive, she finds that the GDPR entails an expansion of the rights of the plaintiff and seeks to address divergences between the pre-existing rules in the Member States, in particular with regard to moral damage, data processor liability, joint liability and representation rights of associations. Milda Mačėnaitė (Tilburg University) focusses on the child-specific rules of the EU GDPR and compares these newly created norms with the existing legal rules for the protection of minors in EU consumer law. She identifies the well-established concepts, justifications and instruments for the protection of minors in EU consumer law and points to possible lessons for the interpretation of the rules in the GDPR. Matilde Ratti (University of Bologna) identifies common features of the regulatory techniques used in data protection and in consumer protection law. Both fields of law seek to protect the weaker subject: they attribute specific rights like the right to withdrawal to the weaker subject and create litigation rules in their favour. However, it should be taken into account that the consumer protection rules aim to balance the contractual interests of the parties while the data protection rules seek to protect a fundamental right.

Widening the view to other legal fields, Davide Mula (European University of Rome) examines the interactions between cloud service contract law and the data protection rules. In this context, he highlights the benefits that the introduction of the right to data portability in Art. 20 of the EU GDPR brings for users of cloud services. Francesco Banterle (University of Milan) explores the extent to which sets of personal data collected for commercial use can be the subject of IPRs, particularly of trade secrets and database *sui generis* rights. He elaborates on the ownership regime set out by the intersection between data protection and IP laws. Addressing the specific issue of targeted advertising, Guido Noto La Diega (Northumbria University) critically reviews current regulatory approaches while developing a specific proposal to effectively empower users with the control of their data. Bianka Maksó (University of Miskolc) analyses the concept of Binding Corporate Rules (BCR) which is one of the novelties in the GDPR. She identifies the commercial and strategic value of personal data and the need for multinational companies to comply with national and European privacy rules in their everyday business, in particular when international data transfers are involved. Maksó then analyses the concept of BCRs, which constitutes an instrument of self-regulation for companies and which seeks to reduce the administrative and financial burdens for companies while assuring their compliance with data protection standards. Heiko Richter (Max Planch Institute for Innovation and Competition, Munich) applies the concept of "private power" to the treatment of personal data by different fields of law in order to achieve an effective and coherent regulation of personal data.

In sum, the identification of shortcomings, common features and possible synergies between different legal fields underlines the need and possible steps for developing a holistic regulatory approach with regard to personal data. Such an integrated approach would result from a trade-off between different legal objectives and values. While developing new data-based innovative products and services is important, it is equally essential to consider the fundamental-rights dimensions of personal data and the protection of privacy. From an institutional perspective, the objectives and rationale of each field of law contemplated should duly be taken into account.

Part I
Fundamentals of Personal Data: Between Personal Property Rights and Regulation

The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right?

Manon Oostveen and Kristina Irion

Contents

1 Introduction 8
2 The Rationale of Fundamental Rights Protection for Privacy and Personal Data 9
2.1 Privacy and Data Protection as Stand-Alone Fundamental Rights 9
2.2 Privacy and Data Protection as Enabling Rights 10
2.3 The Enabling Function of Privacy and Data Protection in the EU 12
3 Big Data, Algorithmic Decision-Making, and Interference with Individual Rights and Freedoms 15
3.1 Big Data and Algorithmic Decision-Making 15
3.2 Interference with Individual Rights and Freedoms 16
3.3 EU Data Protection Law 19
4 Contribution of Data Protection Law to Protecting Individual Rights and Freedoms 21
5 Conclusion 23
References 25

Abstract New technologies, purposes and applications to process individuals' personal data are being developed on a massive scale. But we have not only entered the 'golden age of personal data' in terms of its exploitation: ours is also the 'golden age of personal data' in terms of regulation of its use. In this contribution, we investigate what the objective of fundamental rights protection is as regards privacy and data protection. Understood as an enabling right, the architecture of EU data protection law is capable of protecting against many of the negative short- and long-term effects of contemporary data processing. Against the backdrop of big data applications, we evaluate how the implementation of privacy and data protection rules protect against the short- and long-term effects of contemporary data processing. We

Manon Oostveen completed her PhD research at the Institute for Information Law, University of Amsterdam, and works as an attorney at Netherlands-based law firm Brinkhof.
Kristina Irion is Assistant Professor at the Institute for Information Law, University of Amsterdam.

M. Oostveen (✉) · K. Irion (✉)
Institute for Information Law, University of Amsterdam, Amsterdam, The Netherlands
e-mail: manon.oostveen@brinkhof.com; k.irion@uva.nl

M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law*, MPI Studies on Intellectual Property and Competition Law 28, https://doi.org/10.1007/978-3-662-57646-5_2

conclude that from the perspective of protecting individual fundamental rights and freedoms, it would be worthwhile to explore alternative (legal) approaches instead of relying on EU data protection law alone to cope with contemporary data processing.

1 Introduction

The protection of personal data is justified against the background of protecting individuals' fundamental rights and freedoms, in particular the right to privacy and the new right to the protection of personal data. This chapter articulates the objectives of European Union (EU) data protection law as an enabling human right that renders a discrete contribution to the realisation of a number of other rights and freedoms of the individual. It is argued that EU data protection law's intervention at the stage of processing personal data can produce a number of short- and long-term effects which contribute to preserving individuals' personal autonomy and human dignity.

This research is set against the background of big data applications and algorithmic decision-making, in order to illustrate how both can produce a cascade of effects on individuals' rights and freedoms that goes beyond the core concern of the rights to the protection of private life and personal data. After all, we have entered the 'golden age of personal data' in terms of its exploitation, but also in terms of the regulation of its use. EU data protection law's arsenal of regulatory responses to contemporary challenges of personal data processing has just been upgraded with the adoption of the General Data Protection Regulation (GDPR).[1] It is thus timely to assess the capability of the new Regulation to mitigate the risks of big data applications and algorithmic decision-making for individual fundamental rights and freedoms.

The argument is developed in three steps. First, the rationale of privacy and data protection as *a)* stand-alone fundamental rights, and *b)* enabling rights, which buttress other fundamental rights and freedoms, is mapped out. In the second step, we turn to the EU legal framework on the protection of personal data, and inquire into its discrete contribution to immediate and long-term interference with individuals' fundamental rights and freedoms. Next, after an introduction to big data applications and algorithmic decision-making we provide an overview of the risks for individual fundamental rights and freedoms. Against this background, the discrete contribution of the GDPR's provisions on automated decision-making and profiling are explained and discussed, followed by the conclusions.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1-88.

2 The Rationale of Fundamental Rights Protection for Privacy and Personal Data

2.1 Privacy and Data Protection as Stand-Alone Fundamental Rights

In Europe, individuals' privacy and personal data are protected as fundamental rights in the jurisdiction of the Council of Europe and the European Union, respectively. The right to privacy is protected in Article 8 of the European Convention on Human Rights[2] (ECHR) and Article 7 of the Charter of Fundamental Rights of the European Union[3] (Charter).[4] The right to privacy broadly protects private and family life as well as individuals' home and correspondence in that it attributes a high level of control to individuals. The right to privacy has been interpreted to cover, inter alia, the protection of personal data against unlawful processing.[5]

The Charter's right to the protection of personal data is a 'third generation' fundamental right, elevating data protection to a self-standing right. The protection of personal data's stand-alone value lies in attributing essential tenets of control to individuals when their personal data is processed by third parties. Under the Charter, an interference with the right to privacy is not a precondition for the applicability of the right to the protection of personal data.[6] Nonetheless, as the private life of individuals is increasingly mediated through the internet and online services, situations that trigger privacy concerns now often coincide with the processing of personal data.[7]

The fundamental rights protecting individuals' privacy and personal data are not ends in themselves. Their protection inherently contributes to furthering other individual fundamental rights and freedoms. We call this the *enabling* function of the rights of privacy and data protection.

---

[2] Convention for the Protection of Human Rights and Fundamental Freedoms 1950 (2007/C 303/02).

[3] Charter of Fundamental Rights of the European Union 2009 (OJ C83/02).

[4] Private life and privacy can be and are used interchangeably. See for more details on the usage and interchangeability of the terms González Fuster (2014), particularly p. 81-84 regarding the Convention.

[5] ECHR 26 March 1978, Leander v. Sweden, No. 9248/81, ECLI:CE:ECHR:1994:0310 DEC002325394, para. 48.

[6] For more on the stand-alone value of privacy and data protection, see for example González Fuster (2014); Lynskey (2014); Tzanou (2013).

[7] Recent examples are for instance ECJ, Google Spain and Google, C-131/12, ECLI:EU:C:2014:317; ECJ, Digital Rights Ireland, C-293/12 and C-594/12, *ECLI*:EU:C:2014:238.

2.2 Privacy and Data Protection as Enabling Rights

European legal literature, while making regular references to personal autonomy and human dignity, has not produced many genuine conceptual contributions on the enabling function of the rights to privacy and to data protection.[8] This may be due to the strong constitutional protections in place and the shift of scholarly attention to judicial interpretations of the fundamental rights and the application of data protection law to a variety of diverse activities involving the processing of personal data. In the social sciences, academics are more inclined to inquire into privacy rights as an enabling right, for example in relation to personal autonomy.[9]

Conversely, US legal scholarship continues to argue privacy's important contribution to other individual rights and societal values, resulting in a more profound exploration of the relationship between privacy and other rights and values. Solove rejects the idea that privacy has a unitary value, and instead regards it as a concept that protects a plurality of activities, and is therefore of pluralistic value.[10] In his taxonomy of privacy, Solove touches upon many rights and values that privacy affects, ranging from personal autonomy and freedom of speech to non-discrimination.[11] Richards and Krotoszynski deem privacy indispensable to freedom of speech. Krotoszynski argues that privacy is a precondition for freedom of speech, which makes it also a precondition for democratic self-government.[12] Richards argues the case for intellectual privacy,[13] i.e. the protection of a "*zone to make up our minds freely*", which precedes the actual public expression of ideas and opinions.[14] Roberts takes another angle, by focusing on how privacy facilitates non-discrimination, primarily through obscuring the information necessary to discriminate.[15]

In Europe data protection legislation has often been conceived with the enabling function for individuals' fundamental rights and freedoms in mind. Statutory data protection laws explicitly aim at protecting a number of individuals' fundamental rights and freedoms. In Germany, the Federal Data Protection Law, adopted in 1976, the first national statute of its kind in Europe, broadly aims to protect against the impairment of individual interests through protecting personal data in the course of its processing against being abused.[16] The protected individual interests ("*schutzwürdige Belange des Betroffenen*") certainly include personal integrity and the

[8] There are notable exceptions; see for example Bernal (2014).

[9] E.g. Rössler (2005).

[10] Solove (2008), 98–100.

[11] Solove (2006), 513-514 and 529-530.

[12] Krotoszynski (2016), 175.

[13] Richards (2015).

[14] Ibid., 95.

[15] Roberts (2015), 2173.

[16] Article 1 Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz – BDSG), 27 January 1977.

private sphere, but also other constitutionally protected individual rights and freedoms, namely, freedom of expression, freedom of assembly and association, and freedom of religion.[17] Thus, the formulation of the protected subject-matter has been kept deliberately open for interpretation depending on the circumstances of the processing of personal data.

Similarly, the first French law on the protection of personal data, from 1978, refers to human rights, private life, individual or public liberties ("*droits de l'homme, […] vie privée, […] libertés individuelles ou publiques*") as its objective of protection.[18] The French law took much inspiration from the 1975 *Rapport de la Commission Informatique et Libertés* ("*Le Rapport Tricot*"), which emphasised the close connection between private life and other individual freedoms.[19]

When adopting the 1995 Data Protection Directive, the EU legislature acknowledged that the Directive aims to protect "*fundamental rights and freedoms of natural persons, and in particular their right to privacy*, *with respect to the processing of personal data*".[20] As Dammann and Simitis observe, this creates a functional link between the protection of personal data and fundamental rights and freedoms in general, instead of narrowing its object of protection down to the private sphere.[21] They mention the right to freedom of expression, the right to property and the freedom of profession as individual rights and freedoms that data protection law promotes. Following their commentary, Recital 2 of the Data Protection Directive underscores this general objective when providing that:

> Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals.

The GDPR, which succeeds the Data Protection Directive, entered into force in May 2018. Despite its repeating certain elements of the paragraph above, there is, however, a shift of connotation in Recital (4):

> The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties.

Whereas in the Data Protection Directive it was the data-processing systems which had to respect individuals' fundamental rights and freedoms, it is now the

---

[17] Reh (1978), para. 1-6.

[18] Article 1 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. See Dammann / Simitis (1997), 102.

[19] Rapport de la Commission Informatique et Libertés I, 19 et seq.

[20] Article 1 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data 1995 (OJ L281/31). See also the recurring references to '(fundamental) rights and freedoms' and 'the right to privacy' as separate concepts in the recitals of the Directive.

[21] Dammann / Simitis (1997), 101.

Regulation which has to respect all fundamental rights and observes freedoms and principles of the Charter. This would be alarming if the preamble of EU legislation had binding legal force, which it does not.[22] The GDPR maintains as a broad objective that "*[t]his regulation protects fundamental rights and freedoms of natural persons*" but replaces the particular reference to the fundamental right to privacy with a reference to the right to the protection of personal data (Article 1(2) GDPR). Hence, the European legal culture on the protection of individuals' privacy and personal data has always served to facilitate other fundamental rights and freedoms. The following section sets out to explain how this enabling function is recognised in EU law.

2.3 The Enabling Function of Privacy and Data Protection in the EU

This section will explain how in the 'golden age of personal data' regulating the processing of an individual's personal data can be a proxy of intervention, which directly or indirectly could benefit other individual rights and freedoms. In this section we focus on the enabling function for individual rights and freedoms, leaving collective rights and democratic values, however important, aside. Below we will explain the enabling function in relation to individuals' right to personal autonomy, integrity, and freedom of expression, and in terms of how regulating the processing of personal data vests protection against discrimination, all of which are essential ingredients for the enjoyment of human dignity.

The rights that protect people's private life, thoughts, choice, and expression all operate within the sphere of human dignity. Together with human freedom, respect for human dignity is, in the words of the ECtHR, the "*very essence of the Convention*".[23] Also, the EU "is founded on the indivisible, universal values of human dignity, freedom, [and] equality",[24] and human dignity is protected as an "inviolable right" by the Charter.[25] Personal autonomy can be described as individuals' capability to choose how to live their own lives.[26] As a principle it is considered

[22] ECJ, Criminal proceedings against Gunnar Nilsson, Per Olov Hagelgren and Solweig Arrborn, C-162/97, ECLI:EU:C:1998:554, para. 54; ECJ, Inuit Tapiriit and Others v. European Commission, European Parliament, Council of the European Union, C-398/13 P, ECLI:EU:C:2013:625, para. 64.

[23] ECHR 22 November 1995, CR v. UK, No. 20190/92, ECLI:CE:ECHR:1995:1122JUD002019092, para. 42.

[24] See the preamble of the Charter of Fundamental Rights of the European Union.

[25] Article 1 EU Charter of Fundamental Rights (n 3).

[26] Koffeman (2010), 56; (Personal) Autonomy can be defined in many ways, see for example Dworkin (1988), 3–6, 20 (This chapter follows the conceptualisation based on the case law of the ECHR).

to be a meta-value behind a number of individual fundamental rights and freedoms.

It has been argued that the continental (European) privacy protections are in essence protections of human dignity and personal autonomy.[27] Both offer normative underpinnings of the fundamental rights to privacy and the protection of personal data and are foundations for other fundamental rights and values, which safeguards a sphere of individual choice and freedom. The close relationship between the rights to privacy and personal autonomy comes to the fore in the jurisprudence of the ECtHR.[28] The objective to preserve personal autonomy influences the interpretation of the guarantees of the Convention's right to privacy.[29] The ECtHR has even stated that there is a right to personal autonomy included in Article 8 ECHR.[30] In German constitutional law, the fundamental right to informational self-determination is derived from the protection of human dignity.[31]

Personal autonomy is also a key rationale for instruments in EU data protection legislation, evidenced for example by the principles of consent and the individual's right to access, which aim to confer essential tenets of control over someone's personal data and means to influence the consequences of the processing of those data. The following account offers examples of the enabling effect of personal data protection legislation for the fundamental rights of freedom of expression, freedom of thought and the prohibition of discrimination as protected by the ECHR and the EU Charter.

To begin with, freedom of expression is guaranteed in Article 10 of the ECHR and Article 11 of the Charter. Freedom of expression not only encompasses the right to disseminate information; it also covers the right to hold opinions and freely receive information and ideas. However, today's prevalent monitoring of individual's viewing habits, tracking of online behaviour and extensive profiling could clash with the admittedly negative right to freely receive information. Because users are no longer free to inform themselves without being tracked, this can create a chilling effect for "freely" seeking information. The Court of Justice of the European Union has acknowledged that surveillance, whether by governments or companies, constitutes a serious interference with the fundamental rights to privacy and data protection that has a potentially chilling effect on the freedom of expression.[32]

---

[27] Whitman (2004), 1161; Rössler (2005); Bernal (2014).

[28] Rainey / Wicks / Ovey (2014), 383.

[29] ECHR 29 April 2002, Pretty v. UK, No. 2346/02, ECLI:CE:ECHR:2002:0429JUD000234602, para. 61.

[30] ECHR 10 April 2007, Evans v. UK, No. 6339/05, ECLI:CE:ECHR:2007:0410JUD000633905, para.71; ECHR 24 September 2007, Tysiac v. Poland, No. 5410/03, ECLI:CE:ECHR:2007:0320 JUD000541003, para. 107; ECHR 7 May 2009, Kalacheva v. Russia, No. 3451/05, ECLI:CE:EC HR:2009:0507JUD000345105, para. 27.

[31] BGH, 15 December 1983, I BvR 209, 269, 362, 420, 440, 484/83.

[32] ECJ, Digital Rights Ireland, C-293/12 and C-594/12, ECLI:EU:C:2014:238, para. 28, 37; Judgment (Grand Chamber) of 21 December 2016, joined cases C-203/15 (Tele2 Sverige AB) and C-698/15 (Watson), ECLI:EU:C:2016:970, para. 92 et seq.

With a view to protecting personal autonomy and the right to hold opinions, certain contemporary challenges are not about producing a chilling effect but about personal data-driven techniques of persuasion. Individuals increasingly face personalised messages by private actors but also political organisations, which are designed to persuade and may aim to manipulate individuals' actions from buying new goods and services to casting a vote in democratic elections. Such purposes for the processing of personal data may not be legitimate or may require the individual's explicit consent. However, it is also clear that there is an important threshold for the protection of personal autonomy and the right to hold opinions that would be crossed by practices that are effectively manipulation.

An alternative angle from which to approach these challenges could be the freedom of thought, conscience and religion, which is guaranteed in Article 9 ECHR and Article 10 of the Charter. To date, the relevance of this fundamental right is manifest in protecting religious freedom and—narrowly interpreted—personal convictions.[33] However, as the amount of personal data that is collected about people and their online behaviour increases, so do the possibilities to analyse these data and discover (new) meanings in them.[34] Ways to learn people's thoughts and convictions and to influence them are becoming more advanced. In the future this may become a new frontier for the facilitative function of privacy and data protection, perhaps triggering a renaissance of the fundamental right to freedom of thought.[35]

Personal data processing may lead to various forms of discrimination, intentional or not.[36] Discrimination on grounds such as race, religion, ethnic origin or gender is prohibited by Article 14 of the ECHR and Article 21 of the Charter. Data protection laws can help to mitigate discriminatory practices. This is achieved through giving individuals control over their personal data and providing higher protection for special categories of personal data, i.e. "*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life*" (Article 9 GDPR). The right to privacy also covers certain practices that are closely related to discrimination, such as the negative stereotyping of certain groups.[37]

Recognising the enabling function of the fundamental rights to privacy and personal data protection was close to visionary in the early 1980s. In the light of today's data-intensive technologies the aforementioned risks are likely to grow and situations will arise that will require courts to more clearly argue the enabling functions. In the next step, we become even more concrete when using the contexts of big data and algorithmic decision-making to illustrate the intrinsic connection with

[33] Harris / O'Boyle / Bates / Buckley (2014), 592–594.

[34] On data production and possibilities for analysis in general, see OECD (2015), 133–161; for profiling, see Hildebrandt (2008).

[35] Bublitz (2014), 1-25.

[36] Custers / Calders / Schermer / Zarsky (2013).

[37] ECHR 15 May 2012, Aksu v. Turkey, No. 4149/04 and 41029/04, ECLI:CE:ECHR:2012:0315 JUD000414904, para. 58.

individuals' fundamental rights and freedoms other than the rights to privacy and personal data protection.

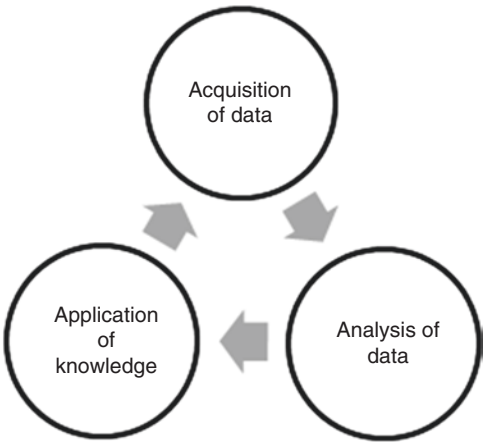
3 Big Data, Algorithmic Decision-Making, and Interference with Individual Rights and Freedoms

3.1 Big Data and Algorithmic Decision-Making

This section uses big data and algorithmic decision-making as a case study to *a)* illustrate how data processing can affect different individual fundamental rights and freedoms, and *b)* show the potential and limitations of the enabling function of the right to data protection, in the guise of contemporary EU data protection law. We commence by explaining the concept of big data and algorithmic decision-making, after which we elucidate its potential effects on individual rights and freedoms. We conclude the section by mapping out how EU data protection law addresses these issues, which is then evaluated in the discussion in the following section.

'Big data' has become a catch-all phrase for applications that involve very large quantities of (personal) data,[38] which are analysed to derive knowledge from it and then used to either target individuals or groups or make general information-based decisions. Big data can thus be regarded as a process consisting of three phases: acquisition, analysis, and application (Fig. 1).[39]

Fig. 1 Big data process



[38] Occasionally big data is based on types of data that do not relate to individuals, such as meteorological data, logistical data, or data about production processes, but often personal data processing is involved.

[39] Oostveen (2016).

In the first phase an organisation collects or acquires (personal) data. Personal data can be collected from individuals directly, for example when a social networking platform asks users to provide them with information. Personal data can also be acquired from data brokers, companies that collect data with the core purpose of selling them to third parties. A third possibility of acquiring data is to combine existing datasets, such as personal data on physical fitness with shopping behaviour, to create new data.

In the second phase of big data, the data is analysed to be able to derive knowledge from it and create for example models or predictions on probabilities of defaulting on payments. The techniques that are used are constantly changing.[40] They include machine learning, which facilitates open-ended explorations for patterns, without clear prior questions or hypotheses being necessary.[41]

In the final phase, the knowledge is applied and algorithmic decisions are made. Based on the models, predictions, or knowledge, individuals can be categorised or clustered, for example to show them different advertisements or decide what interest they should pay on loans. What is important here is to realise that the algorithmic decision is not made solely on the basis of the data from that targeted individual. The decision rests on a limited amount of personal data from this individual, but behind that decision is a wealth of data from other people or sources. The millions of pieces of data that are collected and analysed to *create* the knowledge, models or predictions, are in principle unrelated to the data that are used to *apply* the knowledge, models or predictions in the application phase of big data.

It is also possible that people are not targeted as individuals or groups, but that general decisions are taken that affect their lives nonetheless, such as when governments base policy decisions on big data analytics. The next subsection explicates the immediate effects of big data and algorithmic decision-making and the resultant long-term interferences with individual rights and freedoms.

3.2 Interference with Individual Rights and Freedoms

Undoubtedly, big data as described above can interfere with the rights to privacy and data protection, because of the large-scale collection of personal data and the effect that the processing can have on the private life of individuals. As the collection and processing of personal data intensify and the means to extract knowledge become more sophisticated, the possible spectrum and intensity of interferences increases. However, as this chapter is about the enabling function of privacy and data protection, we focus on big data's detrimental effects on individual rights and freedoms other than privacy and data protection.

First of all, the means used to gather and process individuals' personal data and the lack of transparency surrounding it can exert pressure on the personal autonomy

[40] Custers (2013), 7.

[41] Calders / Custers (2013), 31–38.

and informational self-determination of the individual.[42] Targeting individuals with personalised communications feeds the fear that they will end up in filter bubbles or information cocoons, which would isolate them in a world that consists of limited information that always confirms their beliefs and opinions, without being exposed to diverging information and viewpoints.[43] Whereas people may think they make independent choices and form their opinions autonomously, in such circumstances they are in fact influenced by the limited and customised information that is offered to them. Additionally, people could also be actively persuaded or manipulated through personalisation strategies. Both limiting choices and information as well as actively persuading or manipulating people into a specific choice or decision reduces individuals' personal autonomy. Currently, the effects of personalisation and the steering of opinions and behaviour may be small. But in spite of these instances being small or trivial in terms of their context, because of the opacity surrounding them and their cumulative effects, they could prove harmful for personal autonomy.

Second, big data and algorithmic decision-making can lead to—intentional or unintentional—discrimination.[44] Big data allows for ever more detailed categorisation of people and the customisation of the treatment of individuals. When individuals are treated differently than others on the basis of race, sex, religious beliefs, or other characteristics listed in the Convention and the Charter,[45] this is direct discrimination. But in addition to direct discrimination, big data can cause a more covert kind of discrimination: a seemingly innocent correlation can be a *proxy* for discrimination. This is easily explained through the example of redlining. Redlining refers to the practice in which particular areas or neighbourhoods are denied services, which in practice comes down to denial of services to people of a certain ethnic background as they are the group living in that (generally poor) residential area, leading to discrimination on ethnic grounds.[46] The neighbourhood serves as a proxy for ethnicity. Similarly, correlations in big data can be proxies for prohibited discrimination characteristics. Basing decisions on variables such as pet breed or type of car or dietary requirements may seem innocuous, but they are not if they correlate to ethnic group or religious beliefs. This kind of 'hidden' discrimination is more difficult to uncover than direct discrimination, particularly as numerous variables are used for complex data analysis, as is the case in big data.

The rights to freedom of expression and, potentially, thought are affected by big data in a variety of ways and in different phases of the big data process. As explained above, when people have the feeling that they are under surveillance, be it

[42] Richards / King (2013), 42–43.

[43] Pariser (2012); However, so far no clear evidence about the existence of filter bubbles has been found; see Zuiderveen Borgesius / Trilling / Möller / Bodó / de Vreese / Helberger (2016).

[44] For an extensive (US) analysis, see Barocas / Selbst (2016).

[45] Article 21 European Convention on Human Rights (n 2); Article 14 EU Charter of Fundamental Rights (n 3).

[46] Barocas / Selbst (2016), 689–690.

governmental or corporate, they may alter their behaviour.[47] Surveillance's chilling effect is easily recognised; the mere collection of large amounts of data can be sufficient to affect individuals' right to freely seek and impart information. But freedom of expression also encompasses the rights to hold opinions and to the free reception of information and ideas, and these rights could be compromised by extensive personalisation. Specific characteristics place individuals in groups, which in- or excludes them, in terms of receiving certain information, in the third phase. This potentially limits opportunities to find (new) information and developing ideas and beliefs, which is closely linked to reduced autonomy as described above. The possible harmful effects of big data on freedom of expression and thought thus work two ways: people may self-censor their expression, and their free, unhindered reception of information and forming of thoughts and ideas may be hindered.

In sum, big data and algorithmic decision-making poses risks to several individual rights and freedoms, not just to the rights to privacy and data protection. It has many effects on different rights and freedoms that occur throughout the whole process, as summarised in Fig. 2 below.

But data processing can also affect the lives of individuals *after* the initial processing has occurred. The potential effects of big data, and data processing in

Fig. 2 Big data process including effects on individual rights and freedoms

[47] Richards (2012), 1940–1941, 1952–1953.

general, should be seen as a cascade: it starts with data protection law and privacy, but further on in the process the consequences become more far-reaching for other individual rights and freedoms. This is also what we mean when referring to the 'long-term interferences' of personal data processing. Long-term interference connotes that every instance of personal data processing as applied in automated decision-making alters the course of events, even if at first sight insignificantly, and may yield not only short-term effects, but also long-term interferences. An example of long-term effects: not admitting an applicant to study medicine will inevitably preclude her from becoming a medical doctor in her later life. Thus, the decision changes the course of her career irrevocably and in doing so produces additional effects, such as for example lower income prospects, which will influence the mortgage available to her, etc.[48]

The effects of personal data collection and processing permeate individuals' lives in ways that affect personal autonomy, with significant risks of interfering with individual rights and freedoms across the spectrum, risks that were probably unforeseen at the time of collection. In regulating the beginning of the cascade of effects, the point where personal data are collected and further processed, data protection law has protective potential. The discussion of data protection law's protective potential starts in the following subsection, which summarises what data protection has to offer in the context of (big) data processing and algorithmic decision-making.

3.3 EU Data Protection Law

The data protection law of the EU is composed of key concepts, e.g. the definitions of personal data and individual consent, principles relating to data quality and the requirements of a legal basis for legitimate processing of personal data. The GDPR by and large continues the regulatory approach that has been in place since the Data Protection Directive, such as instituting mechanisms of individuals' control over their personal data and remedies. However, as an EU Regulation, the GDPR will be binding and directly applicable in the Member States (Art. 288 TFEU).

European data protection law protects the fundamental rights and freedoms of individuals by providing them with means to control their personal data, mainly through mandating transparent information and data subject rights. Transparency is achieved by requiring organisations that process personal data to provide the individual with various kinds of information, on for example the identity of the organisation, the type of data processed and the purposes of such processing.[49] The rationale is that this information should enable individuals to assess the intended processing of personal data up front when entering into a commercial transaction or being asked to consent to the processing of their personal data. The right to object

[48] Herpel (2016).

[49] Articles 13-15 GDPR.

to processing and the emphasis on consent as a basis for legitimate personal data processing should enable the individual to set her personal boundaries and differentiate according to data type, organisation or processing context.[50]

In the big data process such means to control the use of one's personal data provide a certain sphere of personal autonomy in that the individual can choose not to be part of a given data processing operation. Moreover, the targeting or personalisation of the application phase can be avoided, although a denial of services may be the result. As such, the control over personal data offered by data protection law addresses the chilling effect that processing can have on freedom of expression and personal autonomy. Further interferences with individual fundamental rights and freedoms are addressed through opportunities to learn about and refuse automated decision-making and, to some extent, personalisation in the application phase.

The provision on automated individual decision-making, including profiling, in Article 22 GDPR has the crucial function to mitigate the risks of big data and automated decision-making for individual rights and freedoms. The GDPR's rules on automated individual decision-making are a prime example of enabling individuals to control their personal data and have agency in the context of automated decision-making. The core of these rules is the right to refuse to be subjected to automated decisions, and this right already existed in the Data Protection Directive. In the GDPR the rules are expanded, most prominently by adding 'profiling' to the provision.[51] To summarise, the GDPR contains five main rules on profiling and automated decision-making: (1) the controller's *obligation to provide information*, (2) the data subject's *right of access to information*, (3) the data subject's right to *object to personal data processing*, (4) the data subject's right to *oppose automated individual decisions*, including profiling, and (5) the *prohibition* on automated decision-making based on *special categories of personal data.*

There clearly is much potential in the combination of information duties with the rights to object and the right not to be subjected to automated decision-making, including profiling, for individual rights and freedoms in big data. Providing individuals with information and giving them the right to object to the processing of personal data as well as automated decisions or evaluative measures strengthens personal autonomy. Individuals have the possibility to decide whether they want to be evaluated or treated differently on the basis of personal aspects, which protects against manipulation. Furthermore, they can demand human intervention in the decision-making process, express their views and challenge the decisions.[52] This right to be heard and judged by humans instead of machines moreover reflects a respect for human dignity. The general possibilities to object and contest decisions, but in particular the prohibition of profiling and decision-making on the basis of special categories of data, can counter instances of direct discrimination in the application phase.

[50] Articles 21 and 6-7 GDPR.

[51] Article 22 GDPR.

[52] Article 22(3) GDPR.

But data protection law is not solely about control and rights of individuals. It is also about obligations of the people or organisations who process the data, and general prohibitions. For example, as explained earlier, discrimination risks are also mitigated by data protection's limitations on the processing of special categories of personal data, such as data on health, ethnicity or religious views.[53] Furthermore, on the basis of the new rules of the GDPR, big data organisations are in principle required to carry out data protection impact assessments, containing among other things descriptions of data flows, risks, safeguards and security measures.[54] Organisations are also under the obligation to take appropriate technical and organisational measures to protect the rights of data subjects. Non-compliance with these provisions is subject to administrative fines.[55] These obligations make organisations aware and responsible for actively safeguarding individuals' rights in practice. How far these duties stretch, and how the general potential of the facilitative role of data protection law plays out in practice with regard to other individual rights and freedoms, is discussed in the ensuing section.

4 Contribution of Data Protection Law to Protecting Individual Rights and Freedoms

It is apparent from the previous section that EU data protection law not only protects the rights to privacy and data protection, but that it has the capacity to also facilitate the protection of other individual rights and freedoms, notably personal autonomy, non-discrimination, freedom of expression and thought, and therefore, ultimately, human dignity. Because of the obligation to inform individuals when their personal data are processed and how this processing takes place, the process should be transparent. Individuals are given an elementary basis for control over their personal data, especially where their consent to the processing activity is required, but importantly also the right not to be subjected to automated decision-making, including profiling. At the same time, organisations must assess their processing to determine risks and precautions, and they are therefore forced to take individuals' rights and interests into account before processing their data. Administrative fines and individual remedies back up these obligations.

Yet, aside from these strong tools, there are a number of weaknesses in the legal data protection framework. To begin with, the scope of data protection law is limited to personal data, meaning data that relate to natural persons who are identifiable through the data.[56] Personal data can be anonymised or non-personal, which also makes their processing unregulated, but their combination with other (personal)

[53] Article 9 GDPR.

[54] Article 35(3)(a) and (7) GDPR.

[55] Article 83(5)(a), (4)(c) GDPR.

[56] Article 4(1) GDPR.

data can affect the lives of individuals.[57] If in general decisions are made in the application phase, algorithmic decisions that do not target individuals but affect their lives nonetheless, would also fall outside the scope of data protection law. In such cases the acquisition and analysis phases could be covered because identifiable data can be processed, whereas the application phase is not. But as the phases are disconnected and the personal data are acquired from other people in the first and second phase, instead of from the individual in the third phase, this affected individual cannot rely on data protection law.

Second, there is scepticism about individual control over data processing as a protection mechanism. Often in a digital environment,[58] but particularly in the context of big data, it is doubtful whether transparency obligations work. Because personal data processing today is ubiquitous and complex, it is questionable whether organisations are always able to adequately inform data subjects about personal data processing, and whether data subjects are capable of assessing the consequences thereof.[59] Moreover, on the internet individuals often interact with near-monopolistic firms, and a denial of services if they do not agree with the conditions regarding personal data sharing. This constrains free choice, or even makes it impossible.[60] Faced with, for example, the automatic refusal of a loan or the impossibility of connecting with others on networks, individuals may easily agree to personal data processing that could lead to discrimination or reduce personal autonomy.

And even if people are offered and have absorbed all information, they still make choices in practice that they claim not to agree with.[61] Reasons are amongst others being tempted by benefits (like being allowed to visit a website, using a service, receiving discounts, or using free apps), not being able to oversee the long-term consequences, or resignation in the idea that privacy and data protection on the internet are a lost cause.[62] People may have the tools to prevent discrimination or chilling effects, and increase personal autonomy, but they may simply not command them. One of the limitations is that privacy management has become a Herculean task for individuals almost impossible to fit into the routines of personal life: reading privacy notices, entering privacy preferences, managing updates in organisations' privacy notices and keeping a general overview over which organisation is processing their personal data for which specific purposes, in addition to being inclined to exercise their rights as data subjects or to turn to the competent data protection authority.[63]

The potential of the automated decision-making rules is limited, as they only apply when a decision has legal effect or when individuals are *similarly significantly affected* by the decision. Second, the decision must be fully automated, i.e. no

[57] Oostveen (2016).

[58] Acquisti (2010); Irion / Luchetta (2013), 35 et seq.

[59] See for example Barocas / Nissenbaum (2014), 2.

[60] Bygrave / Schartum (2009), 160.

[61] Acquisti (2010); Irion / Luchetta (2013), 36 et seq.

[62] Tene / Polonetsky (2013), 67; Rouvroy (2016), 23.

[63] Solove (2013).

human may have played a part in the decision-making process for Article 22 to apply. This means that in practice people's lives may be governed by small and seemingly insignificant algorithmic decision-making, which would, as explained in Sect. 2.2, interfere with personal autonomy, without possible recourse on the basis of Article 22 GDPR. Also, when substantial decisions are based on big data analysis but not applied through automated means, as would be the case when someone is fired on the basis of big data,[64] Article 22 provides no recourse. In the bleakest scenario, the definition of 'profiling' of Article 4(4) GDPR creates another obstacle for the application of Article 22 in the context of big data. Part of the profiling definition is "*the use of personal data to evaluate certain personal aspects relating to a natural person*". And as explained above, the data in the analysis phase often does not qualify as *personal* data. Thus, if the definition of profiling given in Article 4(4) were interpreted narrowly, most big data applications would be beyond the scope of Article 22 *per se.*

It appears to us that the key principles and procedural rights of individuals, which have undergirded EU data protection law since its inception, are more potent to mitigate the long-term risks of big data and algorithmic decision-making than are the specialised provisions on automated decision-making and profiling in the GDPR. The reason is that key principles and procedural rights of individuals are generic, whereas the special rules may not meet big data practice.

5 Conclusion

Where personal data processing is concerned, the discussion of fundamental rights protection often centres on privacy and data protection. After all, these fundamental rights have the most direct connection to the data processing in practice, and the ways in which data processing interferes with these rights are generally quite visible. However, new technologies and data processing applications can affect a range of individual fundamental rights and freedoms, which can subsequently have long-term effects on people's lives.

The protection of privacy and personal data processing with a view to its enabling function for other individual fundamental rights and freedoms has been ingrained in constitutional law in Europe for years, yet this link has not received much attention in the European legal discourse. We deem that this enabling function of privacy and data protection should gain more attention, because of how new data processing developments such as big data and algorithmic decision-making can interfere with individual fundamental rights and freedoms other than privacy and data protection, and the lasting effect this can have on individuals' chances and future. Understood as an enabling right, the architecture of EU data protection law is capable of serving as a proxy for the protection of other individual fundamental rights and freedoms, especially where it provides for appropriate default situations for the handling of

[64] O'Neil (2016), 3-11.

personal data, such as requiring a legal basis and a specific purpose or granting rights to data subjects. The new GDPR certainly strengthens aspects of this core architecture by requiring more accountability as regards compliance with personal data protection standards.

Ironically, certain regulatory innovations introduced by the GDPR to cope with technological advancement and the data-driven economy appear less capable than traditional data protection principles of yielding broad protection for individuals' fundamental rights and freedoms. This chapter has discussed the provisions on automated individual decision-making and profiling, the requirements of which are too narrowly circumscribed to meet the state-of-the-art big data applications. Requiring personal data as an input limits the application of these specific provisions even though automated-decisions are made and individual profiles are created. It seems that the GDPR's specific innovations may not yield as much of an enabling function as the general data protection principles achieve anyhow.

In general, an enabling effect emanates from the GDPR, for example through the control that is bestowed upon individuals with respect to their personal data, and through special protection for sensitive data. However, in practice these effects may be undermined by context-specific barriers. In addition to the examples given above, such as the Herculean task of personal online privacy management,[65] it remains to be seen how the GDPR's standards will work in practice. There is always the risk that the envisaged active protection of individual's rights and freedoms under the law will turn into 'box-checking' and hiding behind formalities in practice.[66] Moreover, data protection authorities' capacities and power to monitor the whole digital personal data processing ecosystem should not be overestimated. Too much optimism in this area equals a lack of attention for the lacunae in the framework of protection of individual rights and freedoms.

In sum, even with privacy and data protection having their stand-alone value and their function as enabling rights, it is time to review possible alternative approaches to the effects of processing personal data. From the perspective of individual rights and freedoms, it is worthwhile to explore how other (legal) approaches can complement privacy and data protection in their protection of individual rights and freedoms in the context of personal data processing. Regulating data processing neutralises part of the negative effects that data processing can have on individual fundamental rights and freedoms, but with respect to the long-term effects on individuals' lives, it is simply not enough.

[65] Solove (2013).

[66] As an example, see how privacy policies are currently often used: they are long, complicated, vague, and almost incomprehensible texts, that seem to be written with compliance and liability in mind, instead of with the aim to provide clear information to data subjects; see Cate / Mayer-Schönberger (2013), 68.

References

Acquisti, A. (2010), The Economics of Personal Data and the Economics of Privacy, Background Paper for OECD Joint WPISP-WPIE Roundtable, 1 December 2010, Paris

Barocas, S. / Nissenbaum, H. (2014), Big Data's End Run Around Procedural Privacy Protections: Recognizing the inherent limitations of consent and anonymity, 31, Communications of the ACM

Barocas, S. / Selbst, A. (2016), Big Data's Disparate Impact, 104 California Law Review 671

Bernal, P. (2014), Internet Privacy Rights: Rights to Protect Autonomy, Cambridge University Press

Bublitz, J.C. (2014), Freedom of Thought in the Age of Neuroscience, 100 Archives for Philosophy of Law and Social Philosophy 1

Bygrave, L. / Schartum, D.W. (2009), Consent, proportionality and collective power, in: P. de Hert / Y. Poullet / S. Gutwirth / (Eds.), Reinventing Data Protection?, Springer

Calders, T. / Custers, B. (2013), What Is Data Mining and How Does It Work?, in: B. Custers / T. Calders / B. Schermer / T. Zarsky (Eds.), Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases, Springer

Cate, F.H. / Mayer-Schönberger, V. (2013), Notice and consent in a world of Big Data, 3 International Data Privacy Law 67, available at: https://academic.oup.com/idpl/article/3/2/67/709124/Notice-and-consent-in-a-world-of-Big-Data

Custers, B. (2013), Data Dilemmas in the Information Society: Introduction and Overview, in: Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases, Springer

Custers, B. / Calders, T. / Schermer, B. / Zarsky, T. (Eds.) (2013), Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases, Springer

Dammann, U. / Simitis, S. (1997), EG-Datenschutzrichtlinie: Kommentar, Nomos

Dworkin, G. (1988), The Theory and Practice of Autonomy, Cambridge University Press

González Fuster, G. (2014), The Emergence of Personal Data Protection as a Fundamental Right of the EU, Springer

Harris, D. / O'Boyle, M. / Bates, E. / Buckley, C. (2014), Harris, O'Boyle & Warbrick: Law of the European Convention on Human Rights, Oxford University Press

Hildebrandt, M. (2008), Defining profiling: a new type of knowledge?, in: M. Hildebrandt / S. Gutwirth (Eds.), Profiling the European Citizen: Cross-Disciplinary Perspectives, Springer

Irion, K. / Luchetta, G. (2013), Online Personal Data Processing and the EU Data Protection Reform, Centre for European Policy Studies, available at: http://www.ceps.eu/book/online-personal-data-processing-and-eu-data-protection-reform

Koffeman, N. (2010), (The right to) personal autonomy in the case law of the European Court of Human Rights, Leiden University

Krotoszynski, R. (2016), Privacy Revisited: A Global Perspective on the Right to be Left Alone, Oxford University Press

Lynskey, O. (2014), Deconstructing Data Protection: The "Added-Value" of a Right to Data Protection in the EU Legal Order, International and Comparative Law Quarterly 569

O'Neil, C. (2016), Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy, Crown

Oostveen, M.A.A. (2016), Identifiability and the applicability of data protection to big data, 6 International Data Privacy Law 299, available at: https://academic.oup.com/idpl/article/6/4/299/2525426/Identifiability-and-the-applicability-of-data

Pariser, E. (2012), The Filter Bubble, Penguin Books

Rainey, B. / Wicks, E. / Clare, O. (2014), Jacobs, White and Ovey: The European Convention on Human Rights, Oxford University Press

Reh, H.J. (1978), Kommentar zum Bundesdatenschutzgesetz, in: S. Simitis / U. Dammann / O. Mallmann / H.J. Reh (Eds.), Kommentar zum Bundesdatenschutzgesetz, Nomos

Richards, N. (2015), Intellectual Privacy: Rethinking Civil Liberties in the Digital Age, Oxford University Press
Richards, N. (2012), The Dangers of Surveillance, 126 Harvard Law Review 1934
Richards, N. / King, J. (2013), Three Paradoxes of Big Data, 66 Stanford Law Review 41
Roberts, J.L. (2015), Protecting Privacy to Prevent Discrimination, 56 William and Mary Law Review 2097
Rössler, B. (2005), The Value of Privacy, Polity Press
Rouvroy, A. (2016), Of Data And Men: Fundamental Rights and Freedoms in a World of Big Data, Bureau of the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [ETS 108]
Solove, D.J. (2013), Privacy Self-Management and the Consent Dilemma, 126 Harvard Law Review 1880
Solove, D.J. (2008), Understanding privacy, Harvard University Press
Solove, D.J. (2006), A Taxonomy of Privacy, 154 University of Pennsylvania Law Review 477
Tene, O. / Polonetsky, J. (2013), Big Data for All: Privacy and User Control in the Age of Analytics, 11 Northwestern Journal of Technology and Intellectual Property 239
Tzanou, M. (2013), Data protection as a fundamental right next to privacy? "Reconstructing" a not so new right, 2 International Data Privacy Law 88, available at: https://academic.oup.com/idpl/issue/3/2
Whitman, J.Q. (2004), The Two Western Cultures of Privacy: Dignity versus Liberty, 113 Yale Law Journal 1151
Zuiderveen Borgesius, F.J. / Trilling, D. / Möller, J. / Bodó, B. / de Vreese, C.H. / Helberger, N. (2016), Should we worry about filter bubbles?, 5 Internet Policy Review

Additional Sources

Herpel, W. (2016), Chaotische Studienplatzvergabe sorgt für Frust, Spiegel Online of 26 June 2016, available at: www.spiegel.de/lebenundlernen/uni/nc-faecher-studienplatz-vergabe-frustriert-studenten-a-1099120.html
OECD (2015), Data-Driven Innovation: Big Data for Growth and Well-Being, OECD Publishing

From Personality to Property?

Revisiting the Fundamentals of the Protection of Personal Data

Andreas Sattler

Contents

1 Introduction 28
2 Individualism and Privacy: Protection Against the Press 29
2.1 The Right to Privacy 29
2.2 Personality Rights 30
3 Dictatorship, Census and Eavesdropping: Protection Against Government 31
3.1 Oppressive Government and Technological Advance 32
3.2 Curious Government and Technological Advance 33
3.3 Disproportionate Balancing of Freedom and Security 34
4 Scoring and Ubiquitous Computing: Protection Against Enterprises 34
4.1 Blurring the Line Between Public and Private Spheres 34
4.2 Efficient Markets and Redistributive Effects of Data Protection 37
5 From Consent to Property: Taboo or Solution? 39
5.1 Autonomous Consent in a World of Information Asymmetries 40
5.2 Towards a Property Right in Personal Data? 41
6 Conclusion 47
References 48

Abstract A holistic and more integrated legal approach to personal data that takes account of economics, social sciences and privacy research constitutes an aspirational challenge. It requires—at the outset—reconsidering the fundamentals on which legal protection of personal data is based. Consequently, this article analyses important milestones in the history of data protection law before concluding with some thoughts on the most radical reformist idea, the introduction of a right to one's data.

Andreas Sattler is Dr. jur., LL.M. (Nottingham) and Senior Lecturer (Akad. Rat a.Z.).

A. Sattler (✉)
Ludwig-Maximilians-University, Munich, Germany
e-mail: andreas.sattler@jura.uni-muenchen.de

M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law*, MPI Studies on Intellectual Property and Competition Law 28, https://doi.org/10.1007/978-3-662-57646-5_3

1 Introduction

The protection of data that relates to an identifiable natural person (hereafter: personal data) has become a battlefield[1] between data protection authorities, attempting to safeguard the constitutionally guaranteed right to informational self-determination, and private companies such as Alphabet and Facebook, which provide their services in exchange for access to personal data and subsequently exploit such data. Besides being used to tailor advertising, access to personal data is increasingly granted as counter-performance (consideration) under contracts for the provision of digital content[2] and in exchange for personalised services. Consequently, the collecting and processing of personal data has become a focal point of the digital economy and the EU's regulatory agenda.[3]

Although the focus of the conference at the Max Planck Institute for Innovation and Competition was rightly on current legal issues that arise in the context of competition, consumer protection and IP law, it is worthwhile to reconsider the fundamentals on which legal protection of personal data is based.

The idea of protecting privacy through law is a concept that originated in the development of individualism in the nineteenth century (Sect. 2); analysis shows that the evolution of the legal protection of personal data under German law was primarily based on a hierarchical concept aimed at protection of individuals from government (Sect. 3). However, when the fundamentals of the law on the protection of personal data were established, the traditional distinction between public and private law was challenged, leading to a unitary regulatory approach, irrespective of whether a data controller is a public agency or a private enterprise (Sect. 4). The underlying principle, to prohibit the processing of personal data unless consent or a statutory permission allows otherwise, is legitimate as far as vertical relationships between citizens and administrative institutions are concerned. However, such a restrictive legal concept of data protection appears increasingly ill-equipped to regulate horizontal data transactions. This article will not suggest an elaborate alternative concept of data protection for the private sector. However, it will conclude with a short reassessment of the most radical reformist idea, the introduction of a "right to one's data" (Sect. 5).

[1] On Hamburg's data protection officer's prohibition of a synchronisation of data between Facebook and WhatsApp: Hamburg Data Protection Officer, Press Release, 27 September 2016. However, just before 25 May 2018 (start of applicability of the European GDPR) Facebook merged the personal data of its Facebook users with the personal data of its Whatsapp users.

[2] Art. 3 (1) of the Proposal of the Commission for a Directive on certain aspects concerning contracts for the supply of digital content, COM/2015/0634 final – 2015/0287 (COD); Langhanke / Schmidt-Kessel (2015), 221.

[3] Digital Single Market Strategy adopted by the Commission on 6 May 2015, COM (2015), 192 final.

2 Individualism and Privacy: Protection Against the Press

The general idea of privacy is not an innovation of the eighteenth or nineteenth century. However, the concept of a legal protection of privacy is a child of industrialisation, having developed in response to its fundamental impact on the development of large cities and the development of an urban bourgeoisie from which modern individualism originates.[4] Monarchs and nobility had the *lèse-majesté* to defend their honour. The urban bourgeoisie, in contrast, had much weaker instruments available to counter the growing reach and influence of the press arising from the rights to free speech and the rapid technical advance that enabled reproduction of text and pictures.[5] Reactions varied according to different legal traditions.[6] While in the US these developments were countered with the concept of a "right to privacy" (Sect. 2.1), German law protected individuality through *Persönlichkeitsrechte* (personality rights) (Sect. 2.2).

2.1 The Right to Privacy

Daily gossip became a business model when newspapers delivered to the urban households superseded the chatter previously voiced in the market-place of agrarian villages. Cities, with their offer of anonymity and consequent decrease in social control,[7] enabled the concealment of personal vices. However, as concealment is no cure for curiosity, it merely increased the prices paid for gossip, thus providing business incentives to peek into other peoples' lives and sell the obtained information.

The lawyer Samuel Warren, himself a Boston celebrity, had learned from first-hand experience that mere ownership of tangibles such as land, bricks and fences—or short: bricks and mortar—could no longer sustain a self-determined private life.[8] To counter the emerging "rainbow press", Warren and his colleague Louis Brandeis argued in favour of a right to be let alone,[9] thus hoping to avoid that "what is whispered in the closet shall be proclaimed from the rooftops"[10]:

> The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some *retreat from the world*, and man, under the refining influence of culture, has become more sensitive to publicity, so that *solitude and privacy* have become more essential to the individual; but modern enterprise and invention have, through invasions upon his

[4] Mallmann (1977), 16 et seq., 32; Posner (1978), 20; Shils (1966), 292; Westin (1968), 22 et seq.

[5] Götting (2008), sec. 2, marginal No. 1 et seq., 16.

[6] For a comparison, see Götting (2008), Part 10.

[7] Mallmann (1977), 19.

[8] See Glancy (1979), 6; Mason (1946), 70; Bloustein (1964), 966.

[9] The term was coined by Cooley (1879), 29.

[10] Warren / Brandeis (1890), 195.

> privacy, subjected him to mental pain and distress, far greater that could be inflicted by mere bodily injury.[11]

Following "The Right to Privacy"—arguably one of the most influential articles written in an American law journal[12]—American courts gradually accepted intrusion, public disclosure, false light and appropriation as sub-categories of privacy protection.[13] While US privacy law predominantly aims to increase individual freedom including the commercialisation of personal facts (right to publicity), German privacy law, by contrast, is strongly focused on the protection of human dignity.[14]

2.2 Personality Rights

Not only for the living, even for the (famous) deceased, "retreat from the world" was compromised by modern enterprise and invention. In 1898 the German Reichsgericht (Imperial Supreme Court) granted protection against two photographers who had broken into the room in which the corpse of the former Imperial Chancellor *Otto von Bismarck* was laid out, taken pictures and sold them to the press. In contrast to French courts, which—in a similar case—could grant protection against the infringement of a person's honour based on Art. 1382 Code Civil,[15] Prussian law provided no such general clause.[16] Instead, the Reichsgericht argued that it impeded the *natürliches Rechtsgefühl* ("natural sense of justice"), if the photographers were entitled to keep the pictures which they had gained through an illegal act.[17] The claim was not granted on rights on protection of a person's honour nor on a concept of privacy but on the infringement of the domestic authority (unlawful trespass), thus drawing it near to property law.[18]

The decision shows that German judges educated in the tradition of Roman law and strict legal positivism were—in contrast to their US counterparts—reluctant to accept any right that could not be derived from a formal Act. Despite strong academic support for personality rights,[19] such protection was only granted indirectly

[11] Warren / Brandeis (1890), 196 (emphasis added).

[12] Prosser (1960), 383; McCarthy (2008), § 1:14.

[13] Prosser (1960), 389 et seq.; McCarthy (2008), § 1:19-24.

[14] Whitman (2004), 1151 et seq.; Wittmann (2014), 50 et seq. and 329 et seq.

[15] Tribunal de la Seine 16 June 1858, Dalloz Jurisprudence Général 1854.3.62 cited by Coing (1988), 77.

[16] In contrast to the law of other continental European countries, the German legislature classified the protection of a person's honour as an objective of criminal law: Götting (2008), sec. 2, marginal No. 2 et seq.

[17] RG, 28 December 1899 – VI 259/99, RGZ 45, 170 (173).

[18] For criticism of such reasoning: Kohler (1900), 208 et seq.

[19] Gierke (1895), 703 et seq.; Gareis (1902), 412 et seq.; Kohler (1880), 129 et seq.; for a summary: Dölemeyer / Klippel (1991), 220.

in cases of criminal offences or infringement of property rights.[20] However, when sec. 22 of the German Act on the Protection of the Copyright in Works of Art and Photographs (KUG) introduced "a right to one's image" in 1907, it did not resort to such reasoning. Instead, sec. 22 KUG was predominantly justified as an instrument to protect the personality of the pictured person and therefore stipulated a direct legal reaction to the challenges faced by individualism due to means of reproduction such as cameras becoming cheaper and smaller.[21]

Even though the Reichsgericht refrained from explicitly accepting other categories of personality rights, it began to grant protection based on general tort law, a very broad interpretation of sec. 22 KUG and copyright law.[22] Starting with the *Leserbrief* judgment of the German Federal Supreme Court (Bundesgerichtshof—BGH) in 1954[23] the protection of personality rights was slowly but steadily expanded.[24]

3 Dictatorship, Census and Eavesdropping: Protection Against Government

As shown, the first legal concepts of personality rights date back to the nineteenth century and concerned protection against a disclosure of personal facts through the press.[25] It was only in the second half of the twentieth century that the processing of information about humans by administrative institutions raised the interest of legal scholars.[26]

Both the first German State Act on the Protection of Personal Data in 1970 (HessDPA) and the first Federal Act on the Protection of Personal Data in 1977 primarily regulated the protection of personal data in relation to governmental authorities (Sect. 3.1). It was not until the 1980s that the law on the protection of personal data became a topic of general public debate. As a result of the protests against the Act of Census, the German Federal Constitutional Court (Bundesverfassungsgericht—BVerfG) interpreted the *Grundgesetz* (German Basic Law) to contain a right to informational self-determination, thus providing for a constitutional warranty that limits governmental curiosity (Sect. 3.2). Since then, the fundamental right to informational

[20] Kohler (1903), 32; also cited by Götting (1995), 18.

[21] On the history of the right to one's image: Götting (1995), 12 et seq.

[22] RGZ 69, 401 – *Nietzsche-Briefe*.

[23] BGHZ 13, 334 = BGH NJW 1904, 1404 – *Leserbrief*.

[24] BGH GRUR 1956, 427 – *Paul Dahlke*; BGHZ 26, 349 = BGH NJW 1958, 827 – *Herrenreiter*; BGH GRUR 1965, 254 – *Soraya*; for an overview see: Götting (2008), sec. 2, marginal No. 15 et seq.

[25] For earlier notions of privacy see: Solove (2006), I-4 et seq.

[26] However, Robert von Mohl und Lorenz von Stein discussed options to restrict government from collecting data in the 19th century; see Geiger (1994), 662.

self-determination has proven to be a dynamic concept able to tackle new technological and political challenges (Sect. 3.3).

3.1 Oppressive Government and Technological Advance

As with other German success stories, the pride that emanates from the fact that in 1970 the German State of Hesse enacted the world's first Act[27] on the protection of personal data[28] risks eclipsing[29] the fact that the Act stems from the experience of a burnt child dreading the fire. German laws on the protection of personal data feed from the same bitter source as the *allgemeine Persönlichkeitsrecht* (general personality right) protected under Art. 2(1) and Art. 1(1) German Basic Law. The city of Frankfurt at the centre of the State of Hesse had been at the heart of what retrospectively became known as the "Generation of 1968", the post-World War II generation that—irrespective of its ambivalent political consequences—can claim to have initiated a process of coming to terms with Germany's oppressive National-Socialist past.[30]

This process and the general public debate had a strong impact on the preparatory works that eventually led to the first Federal Act on Protection of Personal Data (FDPA) in 1977. A preparatory report on the "Fundamentals of Data Protection" mandated by the Federal Ministry for the Interior is written in plain scientific language. However, it uses an example that leaves no ambiguity as regards potential dangers of extensive data collection by government ("Mr. Hans Müller, a Jew").[31]

Although Germany between 1933 and 1945 can on no account be compared to McCarthyism in the 1950s, American academics have identified the oppressive practices conducted by Senator Joseph McCarthy, assisted by the FBI's John Edgar Hoover, as an important experience that facilitated the legal protection of privacy and personal data in the US.[32] The examples of Germany and the US demonstrate that early regulation on data protection was not merely a reaction to technological advance, but was initiated as a response to negative experiences of governmental abuse of personal data, too.

---

[27] Simitis (2014), Introduction, marginal No. 82. For early regulation of aspects of privacy in the USA: Fair Credit Reporting Act (1970), 15 U.S.C. § 1681; Federal Privacy Act (1974), 5 U.S.C. § 552; Buchner (2006), 6 et seq.

[28] Hess. Datenschutzgesetz, 7 October 1970, GVBl. II 1970, 300-10, 621.

[29] According to Hesse's Prime Minister, the Act was additionally triggered by the implementation of new IT systems: Osswald, cited by "Der Spiegel" 20/1971, 10 May 1971, 88.

[30] Creating the new word *Vergangenheitsbewältigung*, which – like zeitgeist – has no equivalent in other languages.

[31] Steinmüller / Lutterbeck / Malmann / Harbort / Kolb / Schneider (1971), 55 et seq.

[32] See Solove (2006), I-20. Pointing out the role of former soldiers and CIA agents who found employment as FBI agents or private detectives: Shils (1966), 297.

3.2 Curious Government and Technological Advance

It remains open to debate whether Joseph and Mary travelled form Nazareth to Bethlehem in 0—or more likely 4 B.C.—because they were honest and law-abiding people, feared strict legal enforcement or were hoping for a tax relief.[33] As Luke[34] informs us, the reason for their burdensome journey was a general census ordered by Caesar Augustus.[35] When in 1982 the German Parliament passed the *Volkszählungsgesetz* (Act on Census)[36] unanimously, it was—on the face of it—less burdensome, as it forced no German citizen to travel to his place of birth for registration. However, the Act provided government with an extensive legal basis to collect and process personal data for statistical reasons. It led to widespread civil opposition.[37]

On 15 December 1983—shortly before the year in which Orwell's prescient "1984" was set—the BVerfG held the *Volkszählungsgesetz* to be void insofar as it allowed the government to collect and process data beyond the means required for a census.[38] In its seminal judgment,[39] the Court interpreted the general personality right guaranteed under Art. 2(1), Art. 1(1) of the German Basic Law to contain a right to informational self-determination. According to the judges, modern techniques of automatic data processing had fundamentally altered the importance of personal data, leading to the insight that "insofar, no trivial data exists"[40] and therefore the right to determine who collects and uses personal data has to rest with each natural person.[41] To safeguard the right to informational self-determination the BVerfG required the legislature to implement procedural and organisational measures to prevent abuse of personal data.[42]

---

[33] In ancient times census was often used to increase tax revenues or allow a head count as preparation for war.

[34] Luke 2:1-5.

[35] The historic relationship between data and census becomes obvious when one considers the name of the Old Testament Book of Numbers (lat. *liber numeri*), which refers to two censuses that are described in the fourth book of Moses.

[36] Gesetz über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung (Volkszählungsgesetz) of 25 March 1982 (BGBl I, 369).

[37] Simitis (1984), 398; Gola (1984), 1155.

[38] BVerfGE 65, 1 = NJW 1984, 419 – *Volkszählung*; for an earlier decision on the limits on governmental data collection: BVerfGE 27, 1 (7) – *Microzensus.*

[39] Describing it as the "Magna Charta" of German data protection law: Hoffmann-Riem (1998), 515.

[40] BVerfGE 65, 1 (45) – *Volkszählung*: ("insoweit […] gibt es kein 'belangloses' Datum mehr").

[41] BVerfGE 65, 1 (43) – *Volkszählung*.

[42] The required measures included a duty to inform the data subject, explain the mode of data processing and eventually delete the personal data: BVerfGE 65, 1 (48 et seq.) – *Volkszählung.*

3.3 Disproportionate Balancing of Freedom and Security

Starting with its judgment on the Act on Census the BVerfG carefully developed further means of protecting individuals against intrusions of government. The court was able to reinforce the right to informational self-determination to the benefit of a person who was a guest of an alleged criminal and therefore became a target of eavesdropping.[43] Furthermore, the BVerfG prohibited governmental agencies from secretly implementing spying software unless they could prove that a superior public interest was seriously endangered and a court order permitted such surveillance. Interpreting the general personality right to guarantee a right to confidentiality and integrity of information-technological systems ("Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme"),[44] the judges showed their willingness to counter tendencies of the government to concede civil liberties in a fight against terrorism and crime.[45]

4 Scoring and Ubiquitous Computing: Protection Against Enterprises

The German legislative decision to regulate the collection and processing of personal data in a single Act, irrespective of whether the controller is an administrative institution or a private enterprise, was based on the assumption that the traditional distinction between public and private spheres should be abandoned (Sect. 4.1). However, such a unitary approach can—if at all—only be justified as a method of redistribution or to protect an allegedly weaker party (Sect. 4.2).

4.1 Blurring the Line Between Public and Private Spheres

The BVerfG's judgment on the Act of Census concerned the relationship between citizens and government and provided no indication that its reasoning should impact the private sector.[46] However, the Court's conclusion that "no trivial data exists"

[43] BVerfGE 109, 279 = NJW 2004, 999 – *Lauschangriff*.

[44] BVerfGE 120, 274 = NJW 2008, 822 – *Online Durchsuchung*.

[45] BVerfGE 130, 151 = NJW 2012, 1419 – *Telekommunikationsdaten*; BVerfGE 133, 277 = NJW 2013, 1499 – *Antiterrordatei*; see: di Fabio (2008), 424 et seq.

[46] Arguably, the introduction leading to the definition of the right to informational self-determination mentions a general "social environment" and contains no direct restriction to public data controllers, BVerfGE 65, 1 (26) – *Volkszählung*. Parts 3 and 4 of the FDPA (1977) included regulation for "Non-Public Data Controllers".

invited data protection authorities and their representatives to suggest an application of the right to informational self-determination in the area of private law, too.[47]

Admittedly, such a unitary approach had already been adopted in the FDPA (1977), and it reflected the regulatory zeitgeist. The decade preceding the Court's judgment can be characterised as a transformational period. Social benefits and governmental schemes were extended and the idea of promoting social participation and personal development gained strong political support.[48] The reasoning of the BVerfG in 1983 seems to have strongly relied on the 1971 report on the "Fundamentals of Data Protection" commissioned by the Ministry of the Interior.[49] This report was heavily inspired by social concepts of Niklas Luhmann and of the Frankfurt School of Sociology, in particularly those of Jürgen Habermas.[50]

While sociology might be descriptive as regards social realities, and is therefore a valuable auxiliary tool in the process of decision-making, it cannot substitute normative decisions.[51] Retrospectively, the aforementioned report seems to lack a clear distinction between descriptive social analysis and normative demands for regulation. The report's authors claim, as one of their key findings, that the traditional separation of public and private spheres should no longer serve as a starting point for regulation.[52] Although the report continued to distinguish between public and non-public data controllers for reasons of readability, it did not analyse in detail whether or not the same regulation was justified in the private sector.[53] Instead, the authors were convinced that the "right to self-determination as regards individual information"[54] was protected under German Basic Law and should be applicable in relation to private data controllers, too.[55]

---

[47] Against the application in the private sector: Zöllner (1985), 3; Meister (1986), 173; Baumann (1986), 1; Ehmann (1988), 301; Wente (1984), 1447.

[48] From 1969 to 1982 so-called social-liberal coalitions led by the social democrats Willy Brandt and Helmut Schmidt governed the Federal Republic of Germany.

[49] Notably, the term right to informational self-determination is very similar to the report's wording: "right to self-determination as regards individual information" ("Recht auf Selbstbestimmung über Individualinformationen"), Steinmüller / Lutterbeck / Malmann / Harbort / Kolb /Schneider (1971), 93.

[50] Habermas (1962); Luhmann (1965) and (1966).

[51] Therefore reluctant to derive any direct legal implications from her "Privacy as Contextual Integrity": Nissenbaum (2004), 119 and 136. Probably with the aim to directly derive regulatory interventions from such social analysis: Pohle (2016) 620 et seq.

[52] "Der Dualismus Staat – Gesellschaft wird den Problemen unserer Zeit nicht mehr gerecht. Vielmehr sind beide Bereiche untrennbar zu einem Gemeinwesen verschmolzen […]", ("The dualism of state – society cannot cope with the challenges of our time. In contrast, both sectors have inseparably been melted into one commonwealth"), Steinmüller / Lutterbeck / Malmann / Harbort / Kolb / Schneider (1971), 35.

[53] Research on the US concept of a right to privacy was mentioned, but rejected as "only of limited use" to the German discussion due to its focus on civil law ("für die deutsche Diskussion nur bedingt verwendbar wegen des starken zivilistischen Ansatzes"), Steinmüller / Lutterbeck / Malmann / Harbort / Kolb / Schneider (1971), 37.

[54] Ibid., 93.

[55] Ibid., 41 and 137 et seq., citing Nipperdey (1962), 17 and Leisner (1960).

This dissolving of the public and private spheres led to the implementation of a principle of constitutional law in the field of private law.[56] The general prohibition of processing personal data unless consent or statutory permission allows otherwise (*Verbot mit Erlaubnisvorbehalt*) corresponds to the constitutional requirement of a specific enactment of government for each restriction of fundamental rights (*Gesetzesvorbehalt*). Such a concept that is based on fundamental rights and which prohibits the processing of personal data might be justified in relation to governmental data controllers.[57] However, this applicability of fundamental rights was extended to private law, became accepted as a general rule of German data protection law[58] and was subsequently introduced as European law for the protection of personal data. It has thus become the gold standard of European data protection law.[59]

When it was introduced for the first time, this concept contained a major disadvantage: the use of personal data either required the consent of the data subject or a statutory permission. As consent had to be given as a separate declaration in writing,[60] it was so burdensome that the relevance of statutory permissions increased. Consequently, the FDPA had to be amended every time a new technology was developed. Therefore each reform of the FDPA provided for additional justifications as regards transactions with private data controllers.[61] Due to failure to keep pace with technological advance, Parliament eventually decided to introduce general clauses that could justify the use of personal data, while requiring the data controller to take the data subject's interests into consideration. Although such general clauses might facilitate flexibility, they turned the Act into a complex and almost indecipherable body of law, thus increasing legal uncertainty.[62] As a consequence private data controllers—just like administrative institutions—have to balance their own interests against those of the data subject,[63] a Herculean and almost schizophrenic task, especially for start-ups and their legal counsel.[64]

---

[56] As expressed by Walter Schmidt (1974), 247: "Insofern ist das zwingende Privatrecht heute nichts anders als konkretisiertes Verfassungsrecht" ("Insofar the compulsory parts of private law are nothing other than substantiated constitutional law").

[57] The 1971 report justifies its unitary approach towards administrative institutions and private business with the potential "social super power" of private companies Steinmüller / Lutterbeck / Malmann / Harbort / Kolb / Schneider (1971), 138; citing Müller (1964), 161. See also: Schmidt (1974), 247: "Das alles läuft darauf hinaus, den Vorbehalt des Gesetzes aus Gründen des verfassungsrechtlichen Persönlichkeitsschutzes ins Privatrecht auszudehnen".

[58] Sec. 4(1) FDPA (1990), BGBl. Teil I, 2924.

[59] Formerly Art. 7 of the EU Data Protection Directive (95/46/EG) and currently Art. 6(1) European General Data Protection Regulation, (EU) 2016/679.

[60] Sec. 3 No. 2 FDPA (1977).

[61] Simitis (2014), marginal No. 92 ("Regelungskonzept fehlte").

[62] On the advantages and disadvantages of general clauses: Ohly (1997); disappointed as regards the general clauses: Simitis (2014), Introduction, marginal No. 141.

[63] See Art. 6(1) lit.f GDPR.

[64] For similar criticism as regards the right to one's image: Canaris (1989), 169; Helle (1991), 27.

In a nutshell: the German legislature[65] had failed to overcome the uniform regulatory approach taken in the 1970s even though its underlying principle of direct applicability of fundamental rights to the private sector was abandoned decades ago.[66] Attempts to clearly divide public and private social spheres have become very difficult.[67] However, for the time being the separation of private and public *law* remains an essential approach to leave private companies sufficient space for innovation.[68]

4.2 Efficient Markets and Redistributive Effects of Data Protection

In his economic analysis of privacy, Richard Posner explained how a strong legal protection towards privacy might cause (negative) economic effects on the markets for labour and credits.[69] According to Posner it was likely that the beneficiaries of privacy legislation were primarily people with more arrests or criminal convictions, or poorer credit records, than the average person. Finding a relation between bad scores and ethnicity, Posner came to the conclusion that "[if] employers and creditors are unable to use these criteria to sift out poor employment risks or poor credit risks, respectively, a redistribution of wealth from whites to members of these racial and ethnic groups may result."[70]

Irrespective of whether Posner's example and wording is a good choice or not, the actual potential redistributive effects of data protection law can hardly be denied.[71] When the BGH[72] in 1978 accepted a legitimate interest of creditors to include so-called "Schufa clauses" in credit agreements, these potential redistributive

[65] The first EU Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (95/46/EC) was based on a unitary regulatory approach to constitute a European internal market for information; Simitis (2014), Introduction, marginal No. 203 et seq.

[66] Rejecting the direct application of fundamental rights in private sector transactions: Canaris (1984), 203; di Fabio (2001), Art. 2, marginal No. 189 et seq.; Wente (1984), 1446; for a direct application: Hager (1994), 382.

[67] Geuss (2003); Heller (2011); Pohle (2015). Defending the uniform approach as a revolutionary step: Pohle (2016), 618.

[68] Favouring a strict separation between data protection against government and against enterprises: Zöllner (1985), 3; Meister *(*1986), 173. Criticism of legal methodology should not be misinterpreted as a demand for substantial deregulation as regards private data controllers.

[69] Posner (1981), 405 on the labour market: "To the extent that the employee is deficient in one or more of these characteristics, he has an incentive – strictly analogous to the incentive of a seller of goods to conceal product defects – to conceal these deficiencies. That is, he has an incentive to invoke a 'right of privacy' if the employer tries to 'pry' into his private life".

[70] Posner (1981), 407.

[71] Jentzsch (2003); Kim / Wagman (2015), 22.

[72] BGH, 20 June 1978, NJW 1978, 2151 (2152).

effects of data protection were not considered.[73] The judges accepted the advantages of an institutionalised exchange of personal data on the likely ability and willingness of potential debtors to repay.[74] "Schufa" is the acronym for "Schutzgemeinschaft für allgemeine Kreditsicherung", a central credit protection agency founded in 1927 with the aim of improving the evaluation of potential credit defaults.

However, a few years later the court restrained banks and financial institutions from using general terms and conditions in their contracts that allowed for an extensive collection of data and its subsequent transmission to Schufa.[75] According to the BGH[76] such clauses infringed the statutory duty to balance the interests of creditors, the general public and data subjects prior to each transmission of personal data.[77] In 1997 Schufa introduced an extensive scoring system to calculate the probability that a debtor would pay all instalments. Based on facts such as debtor's general payment history, income or area of residence, Schufa arrived at an individual score of creditworthiness for almost all German citizens. Although lawyers argued that Schufa scores merely constituted forecasts based on experience with similar debtors and therefore constituted no personal data,[78] Schufa was and still is criticised for operating an opaque system that has a fundamental impact on a person's ability to access credit.[79]

Responding to demand by data protection authorities, the German Parliament subsequently established some legal conditions for scorings. According to sec. 28b FDPA (2009)[80]—currently sec. 31 FDPA (2018)—a decision on whether or not to conclude, perform or terminate a contract can be based on such a score as long as the latter is the result of scientific statistical methods.[81] However, it prohibits any score that is solely based on the postal addresses of data subjects. If residential addresses are—among other data—used for such scoring, data subjects have to be informed in advance and that notice has to be kept on record. Further, their interests

[73] Nor did the ECJ consider consumer welfare in: ECJ, Asnef-Equifax, C-238/05, ECLI:EU:C:2006:734.

[74] According to the reasoning of the BGH, Schufa led to improved efficiency and increased security, thus enabling the German credit market to function without major risks. Consequently, the Schufa system was held to facilitate less bureaucratic and unobstructed transaction of credit agreements at lower interest rates.

[75] On these practices: Kloepfer / Kutzschbach (1998), 650.

[76] BGH, 7 July 1983, NJW 1984, 436 (437); see also: BGH, 19 September 1985, NJW 1986, 46; BGH, 17 December 1985, NJW 1986, 2505.

[77] Sec. 24 (1) FDPA (1977).

[78] Kamlah (legal counsel of Schufa) (1999), 400; Wuermeling (2002), 3509.

[79] Petri (2003), 235; Kamp / Weichert (2005), 131; Korczak / Wilken (2008), 7.

[80] BGBl. I, 2254.

[81] Art. 22 (2) lit.b GDPR and sec. 31 (1) No.2 FDPA (2018); formerly sec. 28b No.1 FDPA (2009).

are taken account of through a right to obtain information about one's individual credit score[82] and a right to correction[83] and deletion.[84]

While these safeguards help to formally provide data subjects with a minimum degree of control,[85] the practical exercise of such rights shows a different picture. Requiring information or insisting on the deletion of an (incorrect) score may lead to financial disadvantages, as any behaviour that deviates from the average potential borrower will create opportunity costs, reducing the likelihood of a bank to conclude a credit contract with such a troublemaker, and so refraining from the exercise of one's rights might be the rational choice of credit seekers (rational apathy).[86] Consequently, even fierce critics of the current laws on data protection accept that the processing of personal data by banks, credit reporting agencies and insurance companies requires strict regulation.[87]

5 From Consent to Property: Taboo or Solution?

The evolution of the protection of personal data shows that the current legal framework is generally based on a hierarchical perspective between data subjects and data controllers. As the social and economic impact of information technologies increases, so too does the criticism of the current paradigms of German and European data protection law.[88] It might be justified to strictly limit governmental authorities from processing personal data according to the right to informational self-determination. Private law, by contrast, is—at the outset—based on the principle of autonomy, thus stressing the liberty to act freely according to one's will. If viewed from a private law perspective, a regulatory approach that is based on a prohibition of processing personal data raises scepticism. Admittedly, empirical behavioural research on the privacy paradoxon provokes serious doubts as regards the ability of average consumers to rationally consent to the processing of their personal data (Sect. 5.1). While demand for stricter regulation of private data controllers is an intuitive reaction to such behavioural biases, emancipating a right to one's data from the data subject may provide an alternative (Sect. 5.2).

---

[82] Art. 15 (1) lit.h GDPR; formerly sec. 34(2) FDPA (2009).

[83] Art. 16 GDPR; formerly sec. 35(1) FDPA (2009).

[84] Art. 17 (1), (2) GDPR and sec. 31 FDPA (2018); formerly sec. 35(2) FDPA (2009).

[85] Requiring provision of unambiguous information to data subjects as regards the conditions required before a negative report is transmitted to Schufa: BGH, 19 March 2015, NJW 2015, 3508 – *Schufa-Hinweis*.

[86] On the de facto compulsion to accept Schufa clauses: Buchner (2006), 117 et seq.

[87] Bull (2015), 41 et seq.

[88] Bull (2015), 55/71; (2006) 1817; Härting (2015), 3284; Härting / Schneider (2011), 63; Schneider (2014), 225.

5.1 Autonomous Consent in a World of Information Asymmetries

Information on the functioning of cookies, digital fingerprints and other methods of tracking is easily accessible. Nevertheless, even basic understanding of the processing of personal data and the scope of given consent remains a black box for digital natives and non-natives alike.[89] As knowledge of the business models of international data intermediaries[90] grows, data subjects are realising to an increasing extent that digitisation does not run counter to the old adage that there is "no such thing as a free lunch". However, many consumers find it difficult to resist the temptations of immediate (digital) gratification.

Various information asymmetries and biases have already been analysed by means of behavioural economics.[91] Empirical research has raised doubts whether the ticking of a box under a lengthy "declaration on data protection" comes close to anything worth being interpreted as an informed and conscious consent.[92] Thus, consent given prior to accessing a website or downloading an app seems to resemble transactions between explorer and native in the sixteenth century rather than an enlightened declaration of long-term intent. Taken to the extreme: access to personal data, the "gold of the 21st century", is occasionally traded for sparkling glass beads such as the "unsäglich kleinen Münze der gegenwärtigen Techno-Musik" ("outrageously small change of current techno-music").[93]

It remains difficult to derive any immediate policy recommendation from behavioural research.[94] Acting on the assumption that behavioural biases cannot be overcome by average data subjects, current regulatory approaches rely on concepts of (liberal) paternalism[95] such as information disclosure, restrictive rules on the transfer of sensitive data and collective means of enforcement, including a right for consumer protection associations to sue.[96] Future options range from raising the requirements for valid consent to excluding consent to certain business models. It does not take any power of clairvoyance to predict that the more complex the regulation concerning the collection and processing of personal data becomes,[97] the

[89] McDonald / Cranor (2010); Acquisti / Taylor / Wagman (2016).

[90] Evans / Schmalensee (2007), 151; Rochet / Tirole (2006), 645; Cennano / Santaló (2013); Körber (2016), 303 and 348.

[91] Preibusch / Kübler / Beresford (2012), 33. For an overview: Kokolakis (2016); Hermstrüwer (2016), 316 et seq.

[92] Hoeren (2011), 145.

[93] In reference to Rehbinder / Peukert (2015), marginal No. 271, who use this phrase with regard to the level of creativity required in copyright law (translation by author).

[94] Acquisti / Taylor / Wagman (2016); Kerber (2016a), 646.

[95] Sunstein / Thaler (2009), 4 et seq.

[96] Sec. 2(2) No.11 UKlaG; Art. 76(1) GDPR.

[97] The GDPR includes dozens of opening clauses thus enabling EU Member States to maintain or introduce national laws on data protection, see: Kühling / Martini (2016), 448 et seq.

more likely an industry-driven reduction of the level of protection becomes, and the louder the demand to establish a right to one's data will be expressed.[98]

5.2 *Towards a Property Right in Personal Data?*

Economists teach us that according to the efficient-market hypothesis, markets will allocate most resources to that position in which they can be used most efficiently.[99] Therefore, under perfect market conditions without information asymmetries, assigning resources through law will merely have an impact on the transaction costs, the time required for such allocation and—most important—the decision of who receives a chance to benefit from that allocation. Thus, from a theoretical economic perspective, property rights are primarily a method of originally assigning resources to individuals before the market mechanism starts to reallocate.

Despite reluctance among legal scholars to treat personal data as any other resource and leave its allocation entirely to market mechanisms, and although personal data has not been given property right status, markets have, nevertheless, been quick at allocating it. Whether the result of that allocation is flawed, due to illegal abuses of dominant market position[100] or based on information asymmetries and behavioural biases, is the subject of a multi-disciplinary discussion including many legal fields, from contract, tort and consumer protection law to the laws on monopolies and unfair competition. Against this backdrop the most radical reformist idea, the introduction of a right to one's data, might develop into a realistic option.

This article can neither deliver a comprehensive theory of a property right in personal data nor define the term property.[101] However, a cursory consideration of some underlying principles of property rights shows that the law has already evolved personal data into a semi-economic right (Sect. 5.2.1). Two current inconsistencies of European law illustrate that a licensable right to personal data could tackle some challenges of digitisation (Sect. 5.2.2) and that reference to copyright law might open up a promising field of future research (Sect. 5.2.3).

[98] For the exact opposite reaction, a tendency to abandon privacy altogether Heller (2011).

[99] Fama (1970), 383 et seq.

[100] See Bundeskartellamt (engl.: German Federal Cartel Office), Press Release on the Preliminary assessment in Facebook proceeding: Facebook's collection and use of data fraom third-party sources is abusive, 19 December 2017.

[101] On the differences between the concept of property rights and absolute rights such as "Eigentum": Häberle (1984), 39 et seq.; Fikentscher (1996), 363.

5.2.1 Economic Rights to Personal Data

Even before the BVerfG interpreted Art. 2(1) and Art. 1(1) of the German Basic Law to contain a right to informational self-determination, proponents of a right to one's data had started to question the fine-meshed net of administrative regulation.[102] Recently, the idea of property rights in personal data has been suggested.[103]

It is a long-established principle of IP law that the degree of transferability or assignability of a right decides on its classification as personality right (*Persönlichkeitsrecht*) or IP right (*Immaterialgüterrecht*).[104] Thus the decision to introduce an assignable right to one's data would partly emancipate such data from the data subject.[105]

A right to one's data could have advantages for the consumers of digital services in particular. It could increase the awareness that some digital offers are not "free of charge" and that access to personal data is granted as a contractual counter-performance (consideration)[106] that is used to generate profits at the "back side" of the two-sided platform market.[107] Furthermore, an introduction of a right to one's data might facilitate the transparency of contractual clauses due to the necessity to explicitly agree on a data licence. Admittedly, such a data licence would not automatically resolve all behavioural biases that impede the process of consent. Clearly, introducing a right to one's data would reinforce the principle of autonomy and partly lift the regulatory burden.[108]

Analysis of the current law shows that personal data is no longer a mere personality right.[109] Instead, economic rights to personal data have already been accepted.

---

[102] Auernhammer (1977), 210; Gusy (1983), 91; Meister (1983), 163; for the debate in the USA, see: Westin (1968), 324 et seq.; against such a property right: Miller (1971), 211.

[103] Ullmann (1999), 209; Beuthien / Schmölz (1999); Kilian (2002), 925; Mell (1996), 81; suggesting a right similar to property ("eigentumsähnlich"): Polenz (2011), marginal No. 61; Kilian (2012), 169 et seq.; Kilian (2014), 205 et seq. For an economic analysis of the advantages and drawbacks of a property right in personal data: Samuelson (2000), 1125; Schwartz (2003), 2056; Lessig (2006), 200 et seq.; sceptical about a property-like approach: Epstein (1978), 461 and Lemley (2000), 1547.

[104] Kohler (1880), 74.

[105] The general possibility of transferability does not predetermine the mode – or better limitations – such transferability is subject to: Forkel (1988), 498 – with reference to an "objectification of aspects of personal rights".

[106] Langhanke / Schmidt-Kessel (2015), 221 et seq.

[107] Evans / Schmalensee (2007), 151; Rochet / Tirole (2006), 645; Cennano / Santaló (2013); Körber (2016), 303, 348.

[108] For a balanced overview: Kilian (2014), 195 et seq.

[109] Though the part of data protection law that aims at the protection of the data subject's personality right has recently been strengthened by the EU Court of Justice (ECJ, Google Spain and Google, C-131/12, ECLI:EU:C:2014:317) through the introduction of a so-called: "right to be forgotten" in Art. 17 GDPR.

The EU General Data Protection Regulation (GDPR)[110] stipulates a right to sue for damages (Art. 82(1) GDPR),[111] a remedy that—retrospectively—has often been a precursor to new property rights.[112] Furthermore, Art. 20 GDPR constitutes a right to portability, i.e., a right to have one's personal data transferred to a new data controller. Adding the free revocability of consent and the monetarisation stemming from the statutory permission to collect and trade addresses for personalised advertising[113] shows that a further evolution towards a right to one's data can hardly be a taboo. However, the rights of data subjects under the GDPR still come up substantially short of the granting of a fully assignable right to one's data.[114]

Prior to an introduction of a right to one's data further research is required. Substantial objections have been expressed to the commercialisation of personality rights,[115] critics fear that an emancipation of personal data could have a negative impact on freedom of speech and social communication.[116] Even if such a right to one's data is constituted, it will remain a challenge to assign rights to access, use and exchange personal data at reasonable transaction costs, as most personal data—not only on social networks—relates to more than one data subject.[117] Surely, an entire bundle of statutory limitations in favour of the public domain including exceptions for research (eg. data mining) and free speech, or even a general "fair use doctrine" would supplement such a right.[118]

5.2.2 Right to One's Data as a Solution to Legal Inconsistencies

Two inconsistencies in the current legal concept lead to major conflicts. Art. 17(1) lit.b GDPR generally obliges data controllers to cease using personal data and delete it if data subjects revoke their given consent, Art. 7(3) GDPR. Being justified due to the constitutional right to informational self-determination,[119] such free revocability

[110] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[111] Prior to 25 May 2018: Art. 21(1) Directive 95/46/EG as ratified in sec. 7 FDPA (2009).

[112] Zech (2012), 71; Peukert (2008), 56.

[113] Art. 6(2) GDPR.

[114] Describing this evolution as "eine Rechtsstellung, die sich bereits zu einer vermögenswerten Position verfestigt hat" ("a legal position that has substantiated to a property-like position") [translation by author]: Kilian (2014), 207. On the assignability of personality rights: Beverley-Smith / Ohly / Lucas-Schloetter (2005), 129 et seq.

[115] Peifer (2002), 326; Zech (2016), 65 et seq.

[116] Klippel (1983), 408; Simitis (1984), 400; Ehmann (1988), 266; Peukert (2000), 710; Götting (2008), 203; Weichert (2001), 1466; Unseld (2011), 987; also sceptical: Ohly (2002), 158 et seq., 414, 431; Ohly (2011), 438; Acquisti / Wagman / Taylor (2016), 41.

[117] Suggesting a data trustee for personal data: Buchner (2006), 277 et seq.

[118] On the relation between IP law and privacy: Liebenau (2016), 285.

[119] The reference to the right to informational self-determination (Art. 2(1), Art. 1(1) German Basic Law) is hereafter also used in the context of the application of the GDPR. However, it has to be

of given consent is not at the disposal of the parties and can thus not be waived by data subjects.[120] However, if the right to informational self-determination and revocability are taken seriously, two inconsistencies arise: First, current law might not sufficiently protect the right to informational self-determination. Second, an extensive protection of personal data leads to conflicts between contract law and data protection law.

First consider the scenario in which data subjects need to insist on their right to informational self-determination not only in relation to their contractual partner, but to each additional (secondary) data controller. As revoking a given consent affects merely the contractual relation between data subject and the first data controller, it remains ineffective as regards all subsequent data controllers down the data wire. The first data controllers might well be obliged to inform the secondary data controller according to Art. 19, Art. 17(1) lit.b GDPR.[121] Nevertheless, it will be for the data subject to chase after the personal data and invoke the statutory rights to information and erasure against each successive data controller[122]—an unreasonable onus that would have been less burdensome for data subjects if more detailed duties to inform data subjects had been introduced.[123] Admittedly, even sub-licences granted under copyright law often survive an invalidity of the original licence.[124] However, when compared to personal data such a copyright licence primarily facilitates economic exploitation and copyright holders may therefore require less protection than data subjects.

A second example of the existing inconsistency, this one a failed attempt to align contract law and data protection law, can be found in the EU Commission's Proposal for a Directive on certain aspects concerning contracts for the supply of digital content (DigiCD-P).[125] According to Art. 13(2b) DigiCD-P the supplier of digital content shall, in the event of contract termination,

---

clarified that this German concept cannot be applied when interpreting the GDPR. Such interpretation will be based on Art. 16 TFEU and Art. 8 and Art. 7 ECHR.

[120] For the German law prior to 25 May 2018: Schaffland / Wiltfang (2016), sec. 4a, marginal No. 27; Simitis (2014), sec. 4a, marginal No. 95; Scheja / Haag (2013), Part 5, E 5, marginal No. 80; see also sec. 6(1) FDPA. Kilian argues that consent is only revocable as long as contractual performance has not already started: Kilian (2014), 212; similar: Gola / Klug / Körffer (2014), sec. 4a, marginal No. 39.

[121] See also recital 37 GDPR.

[122] See Art. 15 GDPR (right to information) and Art. 17 GDPR (right to erasure).

[123] Art. 13a (1) of the EU Parliament's Proposal suggested extended duties to inform data subjects. However, these duties were reduced in the final version of the GDPR: For a (non-official) synopsis of the relevant regulations in the proposals of the EU Parliament and Council see: Comparison GDPR (2015), 124 et seq. For an overall synopsis including the first European Commission proposal and the final "Trilogue" results: Regulation (EU) No XXX/2016 (2015), 253 et seq.; Albrecht (2016), 37.

[124] Spindler (2016), 808.

[125] Commission's Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, COM/2015/0634 final, 9 December 2015; for a more detailed approach: Art. 13a (2) and (3) lit.c, lit.d of the Draft European Parliament Legislative Resolution on the DigiCD-P (27.11.2017).

> refrain from the use of the counter-performance other than money which the consumer has provided in exchange for the digital content and any other data collected by the supplier in relation to the supply of the digital content including any content provided by the consumer *with the exception of* the *content* which has been *generated jointly* by the consumer and others who continue to make use of the content.

The chosen wording suggests that the EU Commission is aware of the possibility that digital content commonly generated by a multitude of users might include material protected under copyright law.[126] However, in the context of social networks such jointly generated "content" will very likely comprise entanglements of personal data, too. The Commission's proposal in Art. 13(2b) DigiCD-P neglects this dilemma.[127] While a consumer might contractually grant a sub-licensable copyright licence to the supplier of digital content, it remains disputable whether or not Art. 13(2b) DigiCD-P contradicts European law on data protection. According to Art. 7(3) GDPR data subjects seem to be prevented from irrevocably consenting to any use of their personal data. Moreover, it is unlikely that a continued use of personal data after termination of the contract for digital content can be justified according to Art. 6(1) lit.f GDPR[128] or any other statutory permission contained in the GDPR.[129]

In summary: while Art. 13(2b) DigiCD-P might contractually require the data subject not to revoke a given consent even after termination of the contract on digital content, contrastingly, Art. 7(3) GDPR seems to guarantee free revocability at any time. According to Art. 3(8) digiCD-P the GDPR prevails. Consequently, it remains open whether revoking one's consent according to the GDPR constitutes—at the same time—a breach of contract, thus entitling the data controller to claims for damages.[130] If "content" in Art. 13(2b) DigiCD-P is interpreted to include personal data required by other users[131]; it would contain a statutory post-contractual duty to allow for a continued use of personal data, irrespective of whether or not a given consent has been revoked. This dilemma can only be resolved if Art. 7(3) GDPR is interpreted to be at the parties' disposal, thus allowing parties to contract out.[132] However, such interpretation would steer personal data away from personality rights and further approximate it towards an economic right to one's data. Whether or not such a diversion from Art. 7(3) GDPR should be possible under general terms and conditions is another question.

---

[126] For criticism that Art. 13(2b) is not even in accordance with sec. 8 of the German Copyright Act: Spindler, (2016), 808.

[127] The European Commission hopes to avoid this inconsistency by simply asserting that in case of conflict European and national laws on data protection take precedence over the DigiCD: Art. 3(8) and recitals 13, 22 and 37 DigiCD-P.

[128] For discussion on Art. 6(1) lit.f GDPR between Parliament and the Council of Ministers: Albrecht (2016), 37.

[129] However, a potential justification could be the opaque Art. 7(4) GDPR.

[130] Strictly against such interpretation: von Westphalen / Wendehorst (2016), 2187.

[131] For such understanding see also the Interinstitutional Document of the Council of the European Union, ST 14827 2016 INIT, 1 December 2016, 11 (No. 29) and recital 37 DigiCD-P.

[132] Sattler (2017), 1041; Sattler (2018).

The Commission's failure to clearly align its proposal for the DigiCD-P with the GDPR—although both are part of one digital agenda—offers a first glimpse at the many difficulties stemming from overlaps of contract law, copyright law and data protection law.

5.2.3 Towards a Dualistic Data Protection Law?

Future research on a right to one's data should review the evolution of copyright or—more precisely—*droit d'auteur* and *Urheberrecht*.[133] Irrespective of whether the dualistic view that distinguishes between economic and moral rights (French *droit d'auteur)* is taken or a monistic concept is preferred (German *Urheberrecht*), surely any future right to one's data would have to emphasise safeguarding personality rights while data subjects increasingly "de-privatise" data.[134] As the evolution of copyright law and trade mark law show, an emancipation of rights that—at least in Germany—were once counted solely among personality rights is hardly a legal innovation.[135] However, such a partial disentanglement from the personality of the entitled individual was based on a steady line of case law rather than a bold Act of Parliament.[136] The greater the variety of entitlements assigned to data subjects, the more likely a dualistic right to one's data incorporating both moral and economic rights will eventually evolve.

For the avoidance of doubt, reference to copyright is not to be misunderstood as a demand for an exclusive right in personal data. Prior to any introduction of such right, further research on its economic impacts are required. So far, there is no evidence that legal incentives are necessary in order to facilitate the generating and trading of personal data.[137] While some scholars associate ownership in personal data with greater legal certainty,[138] others have criticised such an approach as a "mythical view of private property" that could lead to a tragedy of the anticommons. They fear that a property right might stifle the development of infrastructure and services required to access personal data and thus block research and innovation.[139] Indeed, there is strong evidence that a right to one's data could not solely rely on consensual contracts but would require statutory limitations granting non-consensual

[133] For an analysis of similarities and differences between copyright and data protection law: Schwartmann / Hentsch (2015), 226.

[134] Kilian (2014), 197.

[135] For example: Kessen (2011), 175 et seq.; Sattler (2013), 429; Berger (2016), 178 et seq.

[136] Legal history shows that a calculation of damages granted for the infringement of rights of personality based on an analogy of a "licence fee" or the transferability in case of insolvency tend to be early indications of such emancipation: Götting (1995), 50, 128.

[137] Sceptical as regards non-personal data generated by machines and sensors (industrial data): Kerber (2016b), 998.

[138] For an analysis of the different interests involved and supporting ownership in personal medical data: Hall (2010), 631; suggesting a "Data Property of the People" as regards behavior-generated data: Fezer (2017) 356.

[139] Evans (2011), 77 and 106 et seq.

access, too. Future research into a right to one's data should therefore bear in mind that

> [w]here new and wider rights are sought in order to promote technical or commercial innovation (in the various senses of that word), we always have to look carefully at the evidence and we need time to do so, for rights once conceded are very difficult to retract.[140]

The BVerfG's assumption that "no trivial data exists" does not predetermine that all personal data should be subject to the same regulation. Thus future research on a right to one's data needs to consider the variety of personal data and the respective bundle of rights granted. While some sensitive data sits particularly close to the personal sphere and may therefore never be assignable, other personal data may run at such a distance from the data subject's personality[141] that it might be justifiable to partly emancipate it from its subject. Contracts allowing access to and use of one's personal data for particular purposes might generally be an option. However, as any violation of a data subject's personality rights are very context-sensitive,[142] there remains a Damoclean threat to the validity of such contracts on data ("data licences"), thus turning them into an imperilled high-risk transaction.

6 Conclusion

The Industrial Revolution had a fundamental impact on the means and costs of reproducing texts and pictures. Consequently, questions on the methods and degree of protection of privacy arose. Property, or—more precisely—possession of land or houses could no longer safeguard the freedom to "retreat from the world" formerly enjoyed by the rich, powerful and well-known elites. Contrastingly, possession itself has begun to pose major challenges to privacy. The so-called internet of things and its characteristic of ubiquitous computing technically allows for a *de facto* ubiquitous surveillance of the individual.

The right to privacy (US) and personality rights (Germany) were both legal reactions to early technical advances in reproduction. The introduction of information technology to administration led to the first state Act on Data Protection in 1970. The legal research prior to the FDPA (1977) was influenced by theories of sociology that proclaimed a melding of public and private spheres and was pre-determined due to the very negative experience of Germany's National-Socialist past. Later the BVerfG established and defended a right to informational self-determination against governmental tendencies to compromise civil liberties in attempts to cope with crime and terrorism.

Although originally based on a vertical perspective that focused on a relationship between citizens and administrative institutions, both German and European data

[140] Cornish (2001), 29.

[141] Image used by: Hubmann (1967), 133.

[142] As a result, Becker suggests a right to end-user devices that do not collect personal data. Becker (2016), 826 and (2017), 382 et seq.

protection law applies the same legal principles to data transactions between data subjects and private data controllers (horizontal perspective). While justified as regards administrative data controllers, the horizontal relationship between natural persons and enterprises is—despite many exemptions due to informational, social and economic asymmetries—traditionally based on the principle of autonomy.

Empirical behavioural research has shown a whole range of biases that influence the cognitive process of consent. Such biases, at the one hand, may justify instruments of liberal paternalism that are applied to strengthen data subjects' ability to protect their personal data. A true empowerment of data subjects, on the other hand, could be facilitated by introducing a dualistic right. Such a right—insofar similar to early copyright law—could be property-like and accept that personal data has already been commercialised to some degree. A legal framework for licences on personal data could help enable data subjects to economically profit from the use of their data. At the same time, the kinds of major inconsistencies and the lack of alignment between contract law, copyright law and data protection law that plague the GDPR and the European Commission's DigitCD-P could be avoided. As personal data emanates in great variety and is highly context-sensitive, a right to one's data should—again similar to moral rights of early copyright law—not exclude strong personality rights and vigorous enforcement hereof.

References

Acquisti, A. / Taylor, C. / Wagman, L. (2016), The Economics of Privacy, 54 Journal of Economic Literature 442, forthcoming, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580411

Albrecht, P. (2016), The EU's New Data Protection Law – How A Directive Evolved into a Regulation, 32 Computer und Recht International 33, Otto Schmidt

Auernhammer, H. (1977), Das Bundesdatenschutzgesetz, Betriebsberater, RuW

Baumann, R. (1986), BDSG: Plädoyer für die Beibehaltung der Gesetzeseinheit (Erwiderung auf Zöllner), 3 Recht der Datenverarbeitung 1, Datakontext

Becker, M. (2016), Schutzrechte an Maschinendaten und die Schnittstelle zum Personendatenschutz, in: W. Büscher / J. Glöckner / A. Nordemann / C. Osterrieth / R. Rengier (Eds.), Festschrift für Karl-Heinz Fezer zum 70. Geburtstag – Marktkommunikation zwischen Geistigem Eigentum und Verbraucherschutz, 815, C.H. Beck

Becker, M. (2017), Reconciling Data Privacy and Trade in Data – A Right to Data-avoiding Products, 9 Intellectual Property Journal 371, Mohr Siebeck

Berger, C. (2016), Verkehrsfähigkeit digitaler Güter, 8 Intellectual Property Journal 170, Mohr Siebeck

Beuthien, V. / Schmölz, A. (1999), Persönlichkeitsschutz durch Persönlichkeitsgüterrecht, C.H. Beck

Beverley-Smith, H. / Ohly, A. / Lucas-Schloetter A. (2005), Privacy, Property and Personality, Civil Law Perspectives on Commercial Appropriation, Cambridge University Press

Bloustein, E. (1964), Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser, 39 New York University Law Review 962

Buchner, B. (2006), Informationelle Selbstbestimmung im Privatrecht, Mohr Siebeck

Bull, H.-P. (2006), Zweifelsfragen um die informationelle Selbstbestimmung – Datenschutz als Datenaskese?, 59 Neue Juristische Wochenschrift 1617, C.H. Beck

Bull, H.-P. (2015), Sinn und Unsinn des Datenschutzes, Mohr Siebeck
Canaris, C.-W. (1989), Grundrechtswirkungen und Verhältnismäßigkeitsprinzip in der richterlichen Anwendung und Fortbildung des Privatrechts, 30 Juristische Schulung 161, C.H. Beck
Canaris, C.-W. (1984), Grundrechte und Privatrecht, 184 Archiv für die civilistische Praxis 201, Mohr Siebeck
Cennano, C. / Santaló, J. (2013), Platform competition: Strategic trade-offs in platform markets, 34 Strategic Management Journal 1331, Wiley
Coing, H. (1988), Die Entwicklung des Persönlichkeitsrecht im 19. Jahrhundert, in: A. Kaufmann (Ed.), Rechtsstaat und Menschenwürde, Festschrift für Werner Maihofer zum 70. Geburtstag, 75, Klostermann
Cooley, T. (1879), Treatise on the Law of Tort, Callaghan
Cornish, W. (2001), The Expansion of Intellectual Property Rights, in: G. Schricker / T. Dreier / A. Kur (Eds.), Geistiges Eigentum im Dienst der Innovation, 22, Nomos
Di Fabio, U. (2001), in: T. Maunz / G. Dürig (Eds.), Kommentar zum Grundgesetz, C.H. Beck
Di Fabio, U. (2008), Sicherheit in Freiheit, 61 Neue Juristische Wochenschrift 421, C.H. Beck
Dölemeyer, B. / Klippel, D. (1991), Der Beitrag der deutschen Rechtswissenschaft zur Theorie des gewerblichen Rechtsschutzes und Urheberrechts, in: F.-K. Beier / A. Kraft / G. Schricker / E. Wadle (Eds.), Festschrift zum 100jährigen Bestehen der Vereinigung für den Gewerblichen Rechtsschutz und das Urheberrecht, 185, VCH Verlagsgesellschaft
Ehmann, H. (1988), Informationsschutz und Informationsverkehr im Zivilrecht, 188 Archiv für die civilistische Praxis 232, Mohr Siebeck
Epstein, R.A. (1978), Privacy, Property Rights, and Misrepresentations, 12 Georgia Law Review 455, available at: http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2233&context=journal_articles
Evans, B. (2011), Much Ado About Data Ownership, 25 Harvard Journal of Law and Technology 69, available at: http://jolt.law.harvard.edu/articles/pdf/v25/25HarvJLTech69.pdf
Evans, D. / Schmalensee, R. (2007), The Industrial Organization of Markets with Two-Sided Platforms, Competition Policy International, available at: http://www.nber.org/papers/w11603
Fama, E. (1970), Efficient Capital Markets: A Review of Theory and Empirical Work, in: 25 Journal of Finance 383, available at: http://efinance.org.cn/cn/fm/Efficient%20Capital%20Markets%20A%20Review%20of%20Theory%20and%20Empirical%20Work.pdf
Fezer, K.H. (2017), Data Ownership of the People. An Intrinsic Intellectual Property Law Sui Generis Regarding People's Behaviour-generated Informational Data, 9 Intellectual Property Journal 356, Mohr Siebeck
Fikentscher, W. (1996), Property Rights und Liberty Rights: Normativer Zusammenhang von geistigem Eigentum und Wirtschaftsrecht, in: Bundesnotarkammer (Ed.), Festschrift Helmut Schippel zum 65. Geburtstag, 563, C.H. Beck
Forkel, H. (1988), Lizenzen an Persönlichkeitsrechten durch gebundene Rechtsübertragung, 90 Gewerblicher Rechtsschutz und Urheberrecht 491, C.H. Beck
Gareis, K. (1902), Das Recht am eigenen Bilde, 7 Deutsche Juristen Zeitung 412, C.H.Beck
Geiger, A. (1994), Datenschutzrechtliche Ansätze im deutschen Konstitutionalismus des 19. Jahrhunderts, 13 Neue Zeitschrift für Verwaltungsrecht 662, C.H. Beck
Geuss, R. (2003), Public Goods, Private Goods, Princeton Paperback
Gierke von, O. (1895), Deutsches Privatrecht, Vol. 1, Allgemeiner Teil und Personenrecht, in: K. Binding (Ed.), Systematisches Handbuch der Deutschen Rechtswissenschaft, Duncker & Humblot
Glancy, D. (1979), The invention of the right to privacy, 21 Arizona Law Review 1, available at: http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1318&context=facpubs
Gola, P. (1984), Zur Entwicklung des Datenschutzrechts im Jahre 1983, 37 Neue Juristische Wochenschrift 1155, C.H. Beck
Gola, P. / Klug C. / Körffer, B. (2014), in: P. Gola / R. Schomerus (Eds.), Bundesdatenschutzgesetz, 12th ed., C.H.Beck
Götting, H. (1995), Persönlichkeitsrechte als Vermögensrechte, Mohr Siebeck

Götting, H. (2008), in: H. Götting / C. Schertz / W. Seitz (Eds.), Handbuch der Persönlichkeitsrechte, C.H. Beck
Gusy, C. (1983), Grundrechtsschutz vor staatlichen Informationseingriffen, 74 Das Verwaltungsarchiv 91, Wolters Kluwer
Habermas, J. (1962), Strukturwandel der Öffentlichkeit: Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft, Luchterhand
Häberle, P. (1984), Vielfalt der Property Rights und der verfassungsrechtliche Eigentumsbegriff, 109 Archiv für öffentliches Recht 36, Mohr Siebeck
Härting, N. (2015), Zweckbindung und Zweckänderung im Datenschutzrecht, 68 Neue Juristische Wochenschrift 3284, C.H. Beck
Härtung, N. / Schneider, J. (2011), Warum wir ein neues BDSG brauchen – Kritischer Beitrag zum BDSG und dessen Defiziten, 1 Zeitschrift für Datenschutz 63, C.H. Beck
Hager, J. (1994), Grundrechte im Privatrecht, 49 Juristen Zeitung 373, Mohr Siebeck
Hall, M. (2010), Property, Privacy and the Pursuit of Integrated Electronic Medical Records, Iowa Law Rev 631, available at: https://law.utexas.edu/wp-content/uploads/sites/25/hall_property_privacy.pdf
Helle, J. (1991), Besondere Persönlichkeitsrechte im Privatrecht, Mohr Siebeck
Heller, C. (2011), Post-Privacy. Prima Leben ohne Privatsphäre, C.H. Beck
Hermstrüwer, Y. (2016), Informationelle Selbstgefährdung, Mohr Siebeck
Hoeren, T. (2011), Wenn Sterne kollabieren, entsteht ein schwarzes Loch – Gedanken zum Ende des Datenschutzes, 1 Zeitschrift für Datenschutz 145, C.H. Beck
Hoffmann-Riem, W. (1998), Informationelle Selbstbestimmung in der Informationsgesellschaft. Auf dem Weg zu einem neuen Konzept des Datenschutzes, 123 Archiv des öffentlichen Rechts 513, Mohr Siebeck
Hubmann, H. (1967), Das Persönlichkeitsrecht, 2nd ed., Böhlau
Jentzsch, N. (2003), The Regulation of Financial Privacy: The United States vs. Europe. European Credits Research Institute, available at: http://aei.pitt.edu/9430/
Kamlah, W. (1999), Das SCHUFA-Verfahren und seine datenschutzrechtliche Zulässigkeit, 2 Multimedia und Recht 395, C.H. Beck
Kamp, M. / Weichert, T. (2005), Scoringsysteme zur Beurteilung der Kreditwürdigkeit – Chancen und Risiken für Verbraucher, available at: https://www.datenschutzzentrum.de/scoring/2005-studie-scoringsysteme-uld-bmvel.pdf
Kerber, W. (2016a), Digital Markets, Data and Privacy: Competition Law, Consumer Law and Data Protection, 65 Gewerblicher Rechtschutz und Urheberrecht International 639, C.H. Beck
Kerber, W. (2016b), A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis, 65 Gewerblicher Rechtsschutz und Urheberrecht International 989, C.H. Beck
Kessen, S. (2011), Die Firma als selbstständiges Verkehrsobjekt, Mohr Siebeck
Kilian, W. (2002), Informationelle Selbstbestimmung und Marktprozesse. Zur Notwendigkeit der Modernisierung des Modernisierungsgutachtens zum Datenschutzrecht, 18 Computer und Recht 921, Otto Schmidt
Kilian, W. (2012), Personal Data: The impact of Emerging Trends in the Information Society. How the marketability of personal data should affect the concept of data protection law, 28 Computer und Recht International 169, Otto Schmidt
Kilian, W. (2014), Strukturwandel der Privatheit, in: H. Garstka / W. Coy (Eds.), Wovon – für wen – wozu. Systemdenken wider die Diktatur der Daten, W. Steinmüller zum Gedächtnis, 195, available at: http://edoc.hu-berlin.de/miscellanies/steinmueller-40657/all/PDF/steinmueller.pdf
Kim, J.-H. / Wagman, L. (2015), Screening incentives and privacy protection in financial markets: A theoretical and empirical analysis, 46 The RAND Journal of Economics 22, Wiley
Klippel, D. (1983), Deliktsrechtliche Probleme des Datenschutzes, 38 Betriebsberater 407, RuW Verlag
Kloepfer, M. / Kutzschbach, G. (1998), Schufa und Datenschutzrecht, 2 Zeitschrift für Multimedia und Recht 650, C.H. Beck

Körber, T. (2016), "Ist Wissen Marktmacht?" Überlegungen zum Verhältnis Datenschutz, „Datenmacht" und Kartellrecht, 4 Neue Zeitschrift für Kartellrecht 303, C.H. Beck
Kohler, J. (1880), Das Autorrecht, Fischer
Kohler, J. (1900), Der Fall der Bismarckphotographie, 5 Gewerblicher Rechtsschutz und Urheberrecht 208, C.H. Beck
Kohler, J. (1903), Das Eigenbild im Recht, Guttentag
Kokolakis, S. (2016), Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon, Computers & Security, available at: https://www.researchgate.net/publication/280244291_Privacy_attitudes_and_privacy_behaviour_A_review_of_current_research_on_the_privacy_paradox_phenomenon
Korczak, D. / Wilken, M. (2008), Scoring im Praxistest: Aussagekraft und Anwendung von Scoringverfahren in der Kreditvergabe und Schlussfolgerungen, available at: http://www.vzbv.de/sites/default/files/mediapics/scoring_studie_15_01_2008.pdf
Kühling, J. / Martini, M. (2016), Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, 27 Europäische Zeitschrift für Wirtschaftsrecht 448, C.H. Beck
Langhanke, C. / Schmidt-Kessel, M. (2015), Consumer Data as Consideration, 4 Journal of European Consumer and Market Law 218, C.H. Beck
Leisner, W. (1960), Grundrechte und Privatrecht, C.H. Beck
Lemley, M. A. (2000), Private Property, 52 Stanford Law Review 1545
Lessig, L. (2006), Code and Other Laws of Cyberspace, Version 2.0, Basic Books
Liebenau, D. (2016), What Intellectual Property Can Learn from Informational Privacy, and Vice Versa, 30 Harvard Journal of Law & Technology 285
Luhmann, N. (1965), Grundrechte als Institution. Ein Beitrag zur politischen Soziologie, Dunker & Humblot
Luhmann, N. (1966), Recht und Automation in der öffentlichen Verwaltung, Dunker & Humblot
Mallmann, O. (1977), Zielfunktionen des Datenschutzes, Metzner
Mason, A.T. (1946), Brandeis: A free man's Life, Viking Press
McCarthy, J. (2008), The rights to Publicity and Privacy, Thomson/West
McDonald, A.M. / Cranor, L.F. (2010), Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising, 38th Research Conference on Communication, Information and Internet Policy (Telecommunications Policy Research Conference)
Meister, H. (1983), Das Schutzgut des Datenrechts, 7 Datenschutz und Datensicherung 163, Vieweg
Meister, H. (1986), Schutz vor Datenschutz?, 10 Datenschutz und Datensicherung 173, Vieweg
Mell, P. (1996), Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness, 11 Berkeley Technology Law Journal 1, available at: http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1133&context=btlj
Miller, A.R. (1971), The assault on privacy: computers, data banks, and dossiers, University of Michigan Press
Müller, J.P. (1964), Die Grundrechte der Verfassung und der Persönlichkeitsschutz des Privatrechts, Stämpfli
Nipperdey, H.C. (1962), Grundrechte und Privatrechte, in: Festschrift für Erich Molitor zum 75. Geburtstag 17, C.H. Beck
Nissenbaum, H. (2004), Privacy as Contextual Integrity, 92 Washington Law Review 119, available at: https://www.nyu.edu/projects/nissenbaum/papers/washingtonlawreview.pdf
Ohly, A. (1997), Richterrecht und Generalklausel im Recht des unlauteren Wettbewerbs – ein Methodenvergleich des englischen und des deutschen Rechts, Heymanns
Ohly, A. (2002), Volenti non fit iniuria. Die Einwilligung im Privatrecht, Mohr Siebeck
Ohly, A. (2011), Verändert das Internet unsere Vorstellung von Persönlichkeit und Persönlichkeitsrecht?, 14 Zeitschrift für Medien- und Kommunikationsrecht 428, Otto Schmidt
Peifer, K.-N. (2002), Individualität im Zivilrecht, Mohr Siebeck

Petri, T. (2003), Das Scoringverfahren der SCHUFA, 27 Datenschutz und Datensicherung 631, Vieweg

Peukert, A. (2000), Persönlichkeitsbezogene Immaterialgüterrechte?, 44 Zeitschrift für Urheber- und Medienrecht 710, C.H. Beck

Peukert, A. (2008), Güterzuordnung als Rechtsprinzip, Mohr Siebeck

Pohle, J. (2015), Transparenz und Berechenbarkeit: Die Industrialisierung der gesellschaftlichen Informationsverarbeitung und ihre Folgen, available at: https://www.researchgate.net/publication/271445258_Transparenz_und_Berechenbarkeit_Die_Industrialisierung_der_gesellschaftlichen_Informationsverarbeitung_und_ihre_Folgen

Pohle, J. (2016), Die kategoriale Trennung zwischen „öffentlich" und „privat" ist durch die Digitalisierung aller Lebensbereiche überholt, in: M. Plöse / T. Fritsche / M. Kuhn / S. Lüders (Eds.) Worüber reden wir eigentlich? Festgabe für Rosemarie Will, 612, available at: https://www.hiig.de/wp-content/uploads/2016/12/2016-Pohle-Die-kategoriale-Trennung-zwischen-oeffentlich-und-privat-ist-durch-die-Digitalisierung-aller-Lebensbereiche-ueberholt-2016.pdf

Polenz, S. (2011), Datenschutzrecht, in: W. Kilian / B. Heussen (Eds.), Computerrecht, 29th ed., C.H. Beck

Posner, R. (1978), An Economic Theory of Privacy, AEI Journal on Government and Society 19 available at: https://object.cato.org/sites/cato.org/files/serials/files/regulation/1978/5/v2n3-4.pdf

Posner, R. (1981), The Economics of Privacy, 72 The American Economic Review 405, American Economic Association

Preibusch, S. / Kübler, D. / Beresford, A.R. (2012), Price versus privacy. An Experiment into the competitive advantage of collecting less personal information, available at: https://www.wzb.eu/sites/default/files/%2Bwzb/mp/vam/preibusch-kuebler-beresford__price_versus_privacy_experiment.pdf

Prosser, W.L. (1960), Privacy, 48 California Law Review 383, available at: http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=3157&context=californialawreview

Rehbinder, M. / Peukert, A. (2015), Urheberrecht, 17 ed., C.H. Beck

Rochet, J.C. / Tirole, J. (2006), Two-Sided Markets: A Progress Report, 35 The RAND Journal of Economics 645, available at: http://www.tse-fr.eu/sites/default/files/medias/doc/by/rochet/rochet_tirole.pdf

Samuelson, P. (2000), Privacy As Intellectual Property?, 52 Stanford Law Review 1125, available at: https://cyber.harvard.edu/ilaw/Contract/Samuelson_Full.html

Sattler, A. (2013), Emanzipation des Markenrechts, 5 Intellectual Property Journal 429, Mohr Siebeck

Sattler, A. (2017), Personenbezogene Daten als Leistungsgegenstand. 72 Juristen Zeitung 1036, Mohr Siebeck

Sattler, A. (2018), Personenbezogene Daten als Leistungsgegenstand, in: M. Schmidt-Kessel (Ed.), Telematiktarife und Co. – Versichertendaten als Prämienersatz, forthcoming, Jenaer Wissenschaftliche Verlagsgesellschaft

Schaffland, H. / Wiltfang, N. (2016), BDSG, Erich Schmidt

Scheja, G. / Haag, N. (2013), in: A. Leupold / S. Glossner (Eds.), Münchener Anwaltshandbuch IT-Recht, 3 ed., C.H. Beck

Schmidt, W. (1974), Die bedrohte Entscheidungsfreiheit, 29 Juristen Zeitung 241, Mohr Siebeck

Schneider, J. (2014), Fokus und Raster des Datenschutzes im nicht-öffentlichen Bereich: Hinterfragung und Erneuerung, in: H. Garstka / W. Coy (Eds.), Wovon – für wen – wozu Systemdenken wider die Diktatur der Daten, Wilhelm Steinmüller zum Gedächtnis, 225, available at: http://edoc.hu-berlin.de/miscellanies/steinmueller-40657/all/PDF/steinmueller.pdf

Schwartmann, R. / Hentsch, C.-H. (2015), Eigentum an Daten – Das Urheberrecht als Pate eines Datenverarbeitungsrechts, 32 Recht der Datenverarbeitung 221, Datakontext

Schwartz, P. (2003), Property, Privacy, and Personal Data, 117 Harvard Law Review 2056, available at: http://scholarship.law.berkeley.edu/facpubs/69

Shils, E. (1966), Privacy, its Constitution and Vicissitudes, 31 Law and Contemporary Problems 292, available at: http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3109&context=lcp
Simitis, S. (1984), Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung, 37 Neue Juristische Wochenschrift 398, C.H. Beck
Simitis, S. (2014), Bundesdatenschutzgesetz, 8th ed., Nomos
Solove, D. (2006), A Brief History of Information Privacy Law, in: Proskauer on Privacy, PLI, available at: http://scholarship.law.gwu.edu/faculty_publications/923/
Spindler, G. (2016), Digitale Inhalte – analoges Recht. Braucht das BGB ein Update?, 71 Juristen Zeitung 805, Mohr Siebeck
Steinmüller, W. / Lutterbeck, B. / Malmann, C. / Harbort, U. / Kolb, G. / Schneider, J. (1971), Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern, BT Drs. VI/3826, available at: http://dipbt.bundestag.de/doc/btd/06/038/0603826.pdf
Sunstein, C.R. / Thaler, R.H. (2009), Nudge. Improving Decisions About Health, Wealth and Happiness, Yale University Press
Ullmann, E. (1999), Persönlichkeitsrechte in Lizenz?, 2 Zeitschrift für Medien- und Kommunikationsrecht 209, Otto Schmidt
Unseld, F. (2011), Die Übertragbarkeit von Persönlichkeitsrechten, 113 Gewerblicher Rechtsschutz und Urheberrecht 982, C.H. Beck
Warren, S. / Brandeis, L. (1890), The Right to Privacy, 4 Harvard Law Review 193, available at: http://www.jstor.org/stable/1321160?origin=JSTOR-pdf&seq=1#page_scan_tab_contents
Weichert, T. (2001), Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung, 54 Neue Juristische Wochenschrift 1463, C.H. Beck
Wente, J. (1984), Informationelles Selbstbestimmungsrecht und absolute Drittwirkung der Grundrechte, 37 Neue Juristische Wochenschrift 1446, C.H. Beck
Westin, A.F. (1968), Privacy and Freedom, 25 Washington and Lee Law Review 166, available at: http://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20
Westphalen von, F. / Wendehorst, C. (2016), Hergabe personenbezogener Daten für digitale Inhalte – Gegenleistung, bereitzustellendes Material oder Zwangsbeitrag zum Datenbinnenmarkt?, 71 Betriebsberater 2179, RuW Verlag
Whitman, J.Q. (2004), The Two Western Cultures of Privacy: Dignity Versus Liberty, 113 Yale Law Journal 1151, available at: http://www.yalelawjournal.org/article/the-two-western-cultures-of-privacy-dignity-versus-liberty
Wittmann, P. (2014), Der Schutz der Privatsphäre vor staatlichen Überwachungsmaßnahmen durch die US-amerikanische Bundesverfassung, Nomos
Wuermeling, U. (2002), Scoring von Kreditrisiken, 55 Neue Juristische Wochenschrift 3508, C.H. Beck
Zech, H. (2012), Information als Schutzgegenstand, Mohr Siebeck
Zech, H. (2016), Data as a Tradeable Commodity, in: A. de Franceschi (Ed.), European Contract Law and the Digital Single Market. The Implications of the Digital Revolution, 49, Intersentia
Zöllner, W. (1985), Die gesetzgeberische Trennung des Datenschutzes für öffentliche und private Datenverarbeitung, 2 Recht der Datenverarbeitung 3, Datakontext

Additional Sources

Bundeskartellamt, Press Release, Preliminary assessment in Facebook proceeding: Facebook's collection and use of data from third-party sources is abusive, 19 December 2017, available at: https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/19_12_2017_Facebook.html;jsessionid=55B95381595378663F358148C9F19EDE.1_cid362?nn=3591568

Commission's Proposal for a directive on certain aspects concerning contracts for the supply of digital content, COM/2015/0634 final – 2015/0287 (COD), Publications Office of the European Union, available at: http://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A52015PC0634

Council of the European Union, Interinstitutional File on the Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content: 2015/0287 (COD), 1 December 2016, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_14827_2016_INIT&from=EN

European Commission's Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, 9 December 2015, COM(2015) 634 final, available at: http://ec.europa.eu/justice/contract/files/digital_contracts/dsm_digital_content_en.pdf

Comparison of the Parliament and Council text on the General Data Protection Regulation (Non-official document), available at: https://edri.org/files/EP_Council_Comparison.pdf

Digital Single Market Strategy adopted by the Commission on 6 May 2015, COM(2015) 192 final, Publications Office of the European Union, Publications Office of the European Union, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52015DC0192

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Publications Office of the European Union, available at: http://eur-lex.europa.eu/legal-content/ENG/TXT/?uri=celex%3A31995L0046

Draft European Parliament Legislative Resolution on the Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content (COM(2015)0634 – C8-0394/2015 – 2015/0287(COD), available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0375+0+DOC+XML+V0//EN&language=en

German Commission on Monopolies (Monopolkommission), Competition Policy: The challenge of digital markets, Special Report No. 68, 2015, available at: http://www.monopolkommission.de/images/PDF/SG/s68_fulltext_eng.pdf

Hamburg Data Protection Officer, Press Release on the prohibition of the mass synchronisation of data between Facebook and WhatsApp, 27 September 2016, available at: https://www.datenschutz-hamburg.de/fileadmin/user_upload/documents/Press_Release_2016-09-27_Adminstrative_Order_Facebook_WhatsApp.pdf

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Publications Office of the European Union, available at: http://eur-lex.europa.eu/legal-content/eng/TXT/?uri=CELEX%3A32016R0679

Regulation (EU) No XXX/2016 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (non-official document), available at: https://www.huntonregulationtracker.com/files/Uploads/Documents/EU%20Data%20Protection%20Reg%20Tracker/GDPR-4-column-table.pdf

The Failure of Control Rights in the Big Data Era: Does a Holistic Approach Offer a Solution?

Helena Ursic

Contents

1 Introduction 56
2 The Notion of Control in EU Data Protection Law 58
2.1 Control as the Normative Anchor of Privacy and Data Protection 58
2.2 The Instrumental Dimension of Control in the EU Data Protection Law 60
3 Controlling Personal Data in the Big Data Era 66
3.1 Too Theoretical and Unworkable? 68
3.2 Controlling Anonymous Data 71
4 Discussing Solutions 72
4.1 Strengthening the Right to Information Through the Features of Consumer Protection Law 73
4.2 From Portability to Prosumer Law 75
4.3 Control Rights in Personal Data as a Replication of the Author's Moral Right 77
5 Implications for the Future Policy and for Those Who Will Interpret the New Law: Conclusions 78
References 79

Abstract In the big-data era the increasing, ubiquitous processing of personal data dilutes data protection rights and limits individual control over data. The EU General Data Protection Regulation (GDPR) was intended to mitigate the tensions, but the amended law fell short of being revolutionary. However, the GDPR does incorporate a few novel solutions. Their common point is that they bear strong resemblance to legal instruments in domains other than data protection law. The most striking examples of the interplay can be found in Chapter 2 on data subjects' control rights: data portability, the right to be forgotten and the right to information. This novel

Helena U. Vrabec LLM is researcher and PhD candidate at eLaw, the Centre for Law and Digital Technologies at the Faculty of Law of Leiden University, The Netherlands.

H. Ursic (✉)
eLaw, Centre for Law and Digital Technologies, Leiden Law School, Leiden, The Netherlands
e-mail: h.ursic@law.leidenuniv.nl

M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law*, MPI Studies on Intellectual Property and Competition Law 28, https://doi.org/10.1007/978-3-662-57646-5_4

policy approach implies the potential for a more holistic legal scheme in the EU law in relation to personal data that could eventually lead to a better balance between data subjects' rights and economic needs in the big-data economy.

1 Introduction

Fine words—control, empowerment and autonomy—have been used to describe how individuals should manage their personal data in the data economy. *"The point […] is that users should be able to know, and control, when and to whom they give their information and how it will be used,"* declared former EU Commissioner Neelie Kroes in 2011.[1] However, in the face of recent technological developments and the emergence of new social practices the capacity of individuals to "self-manage" their informational privacy has become very ambiguous.[2]

A Cisco white paper shows how dramatically the Internet traffic grew in the past decade. In 2002, global Internet traffic amounted to 100 Gigabytes per second. In 2016, global Internet traffic climbed up to 20,000 Gigabytes per second.[3] The information overload has reached the point at which consumers' control over data inevitably starts evaporating. According to Moore's law, which predicts an exponential increase of the needed data storage capacity,[4] the "volume problem" for information control efforts will only grow more acute in coming years.[5]

The information outburst and the growing data economy have led to new business models, which have spurred innovation but have also trapped consumers (and their data) within myriad networks, applications and databases.[6] Obscure practices of data processing, sometimes described as a "black box",[7] have often been detrimental to individuals and their fundamental rights, including but not limited to data protection rights. For example, Acxiom, the online data marketplace, has had an essential role in profiling passengers for security risks, but a citizen would never be able to understand how exactly the security score was determined and what proxy was used.[8] As this architecture of choice is neither transparent nor easy to monitor,

[1] Kroes (2011).

[2] Lazaro / La Métayer, (2015), 4.

[3] < https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.pdf >.

[4] European Data Protection Supervisor (2015), 16.

[5] Thierer (2013), 428.

[6] See for example Rubinstein (2012), 1. Due to limited scope, I will not discuss big data and related business practices in further detail. The interested reader may refer to Mayer-Schonberger / Cukier (2013).

[7] Pasquale (2015).

[8] Ibid.

consumers' autonomy and control of an affected individual are inevitably challenged.[9]

The increasing, ubiquitous personal data processing could dilute data protection rights, which is why some authors have argued that it is critical to breathe new life into data protection law.[10] As will be shown in the next sections, many traditional data protection mechanisms are unable to function properly in the big-data era. The consent approach has often been put in the spotlight[11] and control rights also seem to suffer from shortcomings. It seems that simply offering rights and tools to users may not suffice. What is needed is an approach that moves beyond established solutions and seeks for alternative measures.[12] One such alternative is the holistic approach. Holism refers to the theory that certain wholes are to be regarded as greater than the sum of their parts.[13] The paper at hand lends support to this idea by arguing that the interplay of instruments from different fields can make data protection law better equipped for the challenges in the big-data era.

The deficiencies of the current system and the lack of individual control over personal data have been noted by the EU regulators. Big hopes were placed in the recently adopted General Data Protection Regulation (GDPR),[14] but the amended law fell short of the intended revolutionary result.[15] The improvements to the consent approach, which is at the core of conceptualising "privacy as control," were aesthetic at most.[16] The catalogue of data subjects' rights was extended, but it did not make any radical changes to the legal position of a data subject.[17]

However, an interesting observation should be made at this point. In spite of the fact that the catalogue of data subject rights largely builds on the legacy of the 1995 Data Protection Directive (DPD),[18] the GDPR did incorporate some novel solutions in order to refresh the control rights regime. An analysis of the GDPR's Chapter 2 shows that quite a few of them were borrowed from legal areas such as consumer

[9] Other rights that might also be infringed are the right to non-discrimination and due process. See more in Custers (2013), 15 and Crawford / Schulz (2014).

[10] See for example van der Sloot / Broeders / Schrijvers, (2016), 177; Koops (2014), 14.

[11] Custers / van der Hof / Schermer (2014).

[12] Koops (2014), 12-13; See also Thierer (2013), 411; Lynskey (2015), 258.

[13] The concise Oxford Dictionary, Clarendon Press, Oxford, 1990.

[14] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1. The regulation was adopted in May 2016 and will enter in force in May 2018.

[15] See for example van der Sloot / Broeders / Schrijvers, (2016), 177; Koops (2014), 2; Mantelero (2014), 645.

[16] See for example Burton et al. (2016), 3.

[17] See for instance Sartor (2015), 71, in relation to the right to be forgotten. Hildebrandt, on the other hand, places great stress on Articles 22 and 13 of the GDPR, but also notes substantial pitfalls to their successful implementation, Hildebrandt (2012), 51-52.

[18] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] OJ L 281.

protection law, property law and competition law. Along these lines, the GDPR appears to suggest that understanding data protection law holistically could be the light at the end of the tunnel for the EU data protection law. The most striking examples of introducing solutions from other legal disciplines are provisions on data portability, the right to be forgotten and the right to information.

This paper builds on those pioneer holistic ideas by exploring more ways in which data protection overlaps with other legal domains. The focus remains on provisions that relate to data subject control rights. The key research question that the paper strives to answer is *Could the holistic approach offer a solution to the deficiencies of control rights in the big data?*

The paper shall proceed as follows. Section 2 discusses the notion of control in data protection law, exploring its normative and instrumental dimensions. As for the latter, it contains an overview of data subject rights in the upcoming EU Regulation on Data Protection. It explains the nature of individual micro rights and the new setup. Section 3 shows why and how traditional views on personal data protection, in particular data subject rights, can be diluted in the big data economy. It describes legal challenges related to big data and highlights the weaknesses of the traditional system of control rights carried over from the DPD. Finally, Sect. 4 examines the observation that the GDPR indicates a move towards a more holistic approach to the regulation of personal data in the EU digital economy. Three rights, which all exhibit characteristics of several legal disciplines, are examined in more detail: data portability, the right to be forgotten and the right to information. The aim of this section is to answer the key question: could a combination of instruments from different legal fields strengthen the individual's position in the data economy? Section 5 offers conclusions and highlights questions that remain open for further discussion.

2 The Notion of Control in EU Data Protection Law

2.1 Control as the Normative Anchor of Privacy and Data Protection

Without doubt, control over data has always been an argument inherent in discourses on privacy.[19] One of the most well-known conceptualisations is Solove's taxonomy, which highlights six principles, all deeply entrenched in the idea of privacy: the right to be let alone, limited access to the self, secrecy, personhood, intimacy and, last but not least, control over personal information.[20]

[19] Koops et al. (2016), 62-66.

[20] Solove (2002), 1094.

Privacy is a complex notion that consists of several aspects such as physical privacy, privacy of association, privacy of communication and informational privacy.[21] Alan Westin's definition calls attention to its informational aspect: "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to."[22] Modern views are slowly moving away from this traditional understanding of privacy as a multifaceted phenomenon. Instead, they stress informational privacy as an overarching concept entrenched in all privacy aspects.[23] In the wake of the data economy this integral nature of informational privacy is becoming more apparent. A vast number of activities in the private or public sector are connected, in one way or another, with the collection and processing of personal information.

As Westin's definition of informational privacy and Solove's last privacy principle suggest, privacy is a right that helps an individual control her or his life.[24] The idea of privacy as a strong individual claim stretches the meaning of the right so far that it also entails the idea of personal autonomy and dignity.

In the EU legal system control over personal data is seen not only as a facet of the right to privacy but also as an important identifier of the right to data protection. Until the entry into force of the Lisbon Treaty in December 2009, the disconnection between privacy and data protection had been only exceptional and data protection had been used as a synonym for the informational aspect of privacy. On December 1, 2009, the Charter of Fundamental Rights of the EU became legally binding on the EU institutions and on national governments, just like the EU Treaties themselves.[25] The Charter was intended to restate and "strengthen the protection of fundamental rights in the light of changes in society, social progress and scientific and technological developments by making those rights more visible".[26] As a pioneering achievement, Article 8 introduced the right to data protection as a fundamental right in the EU, positioning it on the same level as the guarantee of private and family life and the right to marry and to found a family.[27]

The introduction of data protection as a new right has raised some doubts regarding its relation with privacy and the underlining values, as the GDPR remained silent on normative anchors of the right to data protection.[28] Furthermore, the Court of Justice of the EU (CJEU) has consistently conflated the two rights, which has led to their misinterpretation.[29] However, this does not hinder us from claiming that data

[21] <http://www.rogerclarke.com/DV/Privacy.html>.

[22] Westin (1970), 7.

[23] Koops et al. (2016), 70.

[24] Hijmans (2016), 181.

[25] The Charter was adopted in 2000, but only entered in force in 2009. Charter of Fundamental Rights of the European Union, [2012] OJ C 326.

[26] Ibid., Preamble.

[27] Ibid., Title II, Articles 7-9.

[28] Purtova (2014), 6. However, Purtova missed that recital 7 maintains the connection with the Directive, stating that *"The objectives and principles of Directive 95/46/EC remain sound…"*.

[29] González Fuster (2014), 271; Kokott / Sobotta, (2013), 222.

protection is underpinned by similar or even equal values as the right to privacy, including the objectives of control and self-determination. On the contrary, Lynskey notes that the idea of control is actually strongly entrenched in the right to data protection. Enhanced control should be seen as the new right's defining characteristic.[30] Political documents drafted by EU policy makers during the GDPR negotiations indicate the same conclusion. It would not be an overstatement to claim that the idea of having control over personal data has become a mantra of the European legislature.[31] Moreover, although the GDPR binding text is silent on values behind data protection rules, the recitals are more revealing. On the normative level the concept of control is addressed in Recital 7*: "Natural persons should have control of their own personal data."* The instrumental view of control is explained in Recital 68, which refers to a set of micro rights through which an individual can achieve normative objectives.[32]

2.2 *The Instrumental Dimension of Control in the EU Data Protection Law*

Lynskey describes EU data protection law as a rights-based regime. This is so because, as was established above, the GDPR reflects the fundamental-rights character of the EU regulatory framework.[33] Furthermore, it is rights-based because it grants individuals tangible rights such us the right to object and the right to be forgotten. The GDPR's twofold character is also reflected in Lazaro's observation that data protection encompasses two dimensions—instrumental and conceptual.[34] For both dimensions, individual control over data is an important underlying objective.

In the recently adopted GDPR, the instrumental dimension of control is enshrined in the provisions on individual rights, also referred to as micro rights,[35] data subject's rights,[36] subjective rights[37] or control rights.[38] In their mission to empower

[30] Lynskey (2014), 582.

[31] Lazaro / Le Métayer, (2015), 16. Lazaro lists several documents in which control is mentioned, e.g., the 2013 Proposal for a general data protection regulation, the 2012 Communication from the Commission - Safeguarding Privacy in a Connected World and the 2011 Article 29 Data Protection Working Party's Opinion 15/2011 on the definition of consent.

[32] *"To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller."*

[33] Lynskey (2015), 35.

[34] Lazaro / Le Métayer, (2015), 15.

[35] Ibid., 19.

[36] Levin (2012), 125.

[37] Lynskey (2015), 11.

[38] Ibid., 230.

data subjects these rights are of course not self-sufficient but work alongside the data controllers'[39] obligations.[40] For example, an intrinsic connection can be observed between the duty of a data controller to provide information and micro rights that can be (subsequently) exercised by a data subject. Obviously, the idea of control behind data subject rights is not absolute and can be limited when circumstances so require.[41]

Micro rights are not a novel concept. They were part of several legal documents that preceded the GDPR, constituting the "corpus" of the evolving data protection law. Convention 108,[42] which was one of the first acts that took a general approach towards data protection, listed data subject rights under the title "additional safeguards". The DPD, the predecessor of the GDPR, took a more structured approach, dividing the safeguards from Convention 108 into two groups: the duty to provide information and the remaining rights. The latter group was further split into two sub-groups, the first one labelled "the right of access", including not only the access entitlements but also the right to delete and rectify data, and the second sub-group consisting of the right to object, which can be invoked on compelling legitimate grounds relating to the subject's particular situation, the processing of data relating to the subject or in a situation of behavioural advertising. This structure is in line with the US FTC fair information practice principles,[43] among which the principles of openness and individual participation are of special importance. The openness principle refers to the idea that there should be a general policy of openness about developments, practices and policies with respect to personal data. The individual participation principle on the other hand focuses on traditional data subject rights—access to information and the right to challenge data processing.

The EU data protection reform significantly extended the section on data subject rights. Chapter 2 of the GDPR's rights can be split into three clusters: the first one contains the right to information and the right of access while the remaining two refer to the right to be forgotten and the right to object, respectively. Interestingly, the right to information became part of the data subject rights bundle, which had not been the case under the DPD. Also, very significantly, the GDPR introduced a new right—the right to data portability.

Reasons for the change are straightforward: the GDPR recognised the ineffectiveness of the existing data protection regime and tried to mitigate shortcomings by affording data subjects more control. Some authors stressed that the enhancement of the package of control rights (strengthening and detailing the existing ones, and

[39] "*'Controller' shall mean 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"* (Article 2 of the DPD).

[40] Levin (2012), 125.

[41] See Article 23 of the GDPR (Restrictions).

[42] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37.

[43] Federal Trade Commission (1998), 7.

introducing new ones) could be among the major amendments that the GDPR has brought to the existing data privacy laws.[44] However, their analyses mainly referred to the GDPR's original proposal and not to its final version. Chapter 3 will explore in more detail whether these claims hold water. Before that, the catalogue of control rights will be shortly described.[45]

2.2.1 The Right to Information

The right to be informed is perceived as a static right, but this observation does not render it less important. Just the opposite, receiving the right information is a precondition, a *conditio sine qua non*, for every data subject who wants to exercise his control rights effectively. When there is lack of information, a data subject can be deprived of any meaningful action. This inherent connection between the right to information and other micro rights seems to be the rationale behind the legislature's decision to merge all the entitlements in one, joint chapter.

The right to be informed is the reverse side of the controller's duty to provide adequate information. Like the DPD, the GDPR does not specify how the required information should be conveyed to a data subject. For example, the distinction between actively communicating information about privacy practices and simply making it readily available to data subjects is not addressed and it could be assumed that it is up to a data controller to determine how they will eventually communicate with data subjects.[46] In practice publishing a privacy notice fulfils the information requirement, and this seems to remain the case under the GDPR regime as well.

Whilst the information provision arises primarily from Articles 12–14, the requirements set out in these articles do not cover the full range of information that a data subject actually receives in the course of data processing. As part of his access right, an individual whose information is being collected or stored has a legal right to request the data controller to additionally provide, e.g., information on lifted restriction of processing (Article 18(3)) and information about categories of data (Article 15(1)b).

2.2.2 The Right of Access

If the right to information is the passive side of the coin, the right of access represents the active one. In its most simplistic sense, it gives the data subject the right to demand information about the processing of his personal data. The right originates

[44] Zanfir (2012), 149; Solove (2015).

[45] In Chapter 8, the GDPR grants data subjects additional rights to seek a remedy or to lodge a complaint. However, these rights are not included in the scope of "control rights", as they constitute measures to secure intervention of an authority but do not intend to establish control in its genuine sense.

[46] Jackson (2012), 116.

in the idea of freedom to access, also referred to as freedom of information, which was introduced in the US after World War II in reaction to governmental opacity.[47] While in the past the right of access mainly aimed at controlling the government and autocratic bodies, in the recent years its focus has shifted to the private sector. This is not surprising—if previously the state databases were by far the largest, new data-driven models in the private sector tilt the balance of data ownership in favour of a number of global corporations.[48]

The European legislature considers access an important aspect of individual control, which is also enshrined in the array of information that the GDPR guarantees to an individual.[49] In addition to the catalogue that existed under the DPD, a data subject has a right to receive information about the source of the information, the logic behind automatic processing of information (Article 14) and the authority that can be contacted in relation to data processing. The Regulation contains stricter requirements regarding the time frame within which data controllers must provide the information, and details about the pricing: the first copy is always received for free, while a data subject may be charged a reasonable price for additional copies (Article 15(3)). Nothing prevents a data subject from requesting more (specific) pieces of information. However, those explicitly mentioned in the provision are indispensable for a legitimate and legal data processing, and should be provided by data controllers by default.

2.2.3 The Right to be Forgotten or the Right to Erasure

The right to be forgotten has been one of the most discussed parts of the GDPR proposal. According to Werro, it is a manifestation of the right to oblivion in the digital age and ensures that someone can preclude others from identifying him or her in relation to his or her past.[50] Since this definition focuses less on deletion of data and more on regulating (blocking) secondary data uses,[51] the reference to the idea of control is obvious.

The right to be forgotten, also known as the right to erasure, was a constituent part of the DPD. In this sense, it is not particularly novel.[52] The right gained

[47] Yu / Robinson, (2012), 184.

[48] An interesting agreement has been signed between the Russian Government and Uber. In exchange for enabling Uber to offer services in Moscow, the Russian government secured access to Uber databases. Meyer (2016).

[49] European Commission (2010), 18.

[50] Werro (2009), 291.

[51] Koops (2011), 28.

[52] This might be the reason why the parliament version of the GDPR did not refer to a right to be forgotten: *"The 'right to be forgotten' is a right that is not provided for by this Regulation. By using this term, data subjects are promised a right they in practice do not have. The right to erasure must be as strong as possible and take into account the possible difficulties to remove personal data on the Internet. This should be done by strengthening the right to erasure instead of promising*

importance after the CJEU's landmark ruling in the case *Google Spain,* in which the court opted for a broad interpretation and held that the right to be forgotten applies to search engines.[53] As a basis of the far-reaching decision the Court applied the DPD's provisions on the right to erasure. Although a later GDPR version detailed the scope of the right, it did not introduce any major amendments.

The current diction of the right to be forgotten emphasises the importance of consent and the purpose limitation principle. Article 17(1) explicitly allows data subjects to seek the deletion of data and block further reuse when consent is withdrawn[54] or when the data is no longer necessary in relation to the purposes for which it was collected or otherwise processed. In the Commission's original proposal from 2012, Article 17(2) further stated that the right to be forgotten should follow the data when the data controller has made it public (e.g., by publishing it on a website) or when publication is delegated to a third party. In the latter scenario, the original controller would be held fully responsible for erasure.[55] This is no longer the case under the final GDPR text. In its present form the Regulation only requires controllers to inform third parties if this does not require disproportionate efforts. Van Hoboken is right when he points out that the added value of the updated provision for data subjects who want to see their data deleted is relatively minor.[56]

2.2.4 The Right to Data Portability

Along with the right to be forgotten and the right to modify incorrect or out-dated personal information stored in databases, data portability tends to be a pillar of a stronger, more effective right to *control* over the processing of the data subject's personal data.[57]

The current wording of the right to portability suggests that the right is split into two elements: first, the right to obtain a copy of the respective data for further use and second, the right for individuals to transmit their personal data from one

non-existing rights through misleading titles." AMENDMENTS (4) 1189 – 1492 (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), Draft report Jan Philipp Albrecht (PE501.927v04-00), available at: http://www.europarl.europa.eu/document/activities/cont/201305/20130508ATT65813/20130508ATT65813EN.pdf. *De lege lata* the right to be forgotten has been reflected in the right to objection and erasure. European Commission (N.D.).

[53] EU Court of Justice, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, C-131/1, ECLI:EU:C:2014:317.

[54] Article 7(3) of the GDPR.

[55] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 25 January 2012, available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

[56] Van Hoboken (2013), 14.

[57] Zanfir (2012), 13.

provider to another (Article 20 of the GDPR).[58] The basic idea of the right is that an individual would be able to transfer his or her personal data and other material from one information service to another without hindrance.[59] These industries appear prone to monopolisation, whether as a result of innovation, network effects or even acquisitions, which jeopardises individual control over personal data—individuals simply have no choice.[60] It is believed that portability could enable businesses and individuals to maximise the benefits of big data and to benefit from the value created by the use of their personal data. it would allow them to use the data for their own purposes, or to license the data for further use to third parties, in exchange for additional services, or for cash value.[61] However, portability is only guaranteed under Article 20's strict conditions, requiring that the data in question is processed by automated means and that processing is done on a legal basis of either a contract or an individual's consent. As the rule in Article 20 is new to the fabric of personal data protection,[62] its wording (e.g., the exact meaning of "automated means") is open to interpretation and actual outcomes are difficult to predict.

2.2.5 The Right Not to be Subject to a Decision Based Solely on Automated Processing

This right, explicated in Article 22(1), makes sure that an individual has the right not to be subject to a decision based solely on automated processing, including profiling, as long as it produces legal effects concerning him or her or similarly significantly affects him or her. This right does not apply to processing which has a legal basis in a contract, an individual's consent or a legal obligation. However, in these cases a data controller must implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision (Article 22(3)).

A fully automated decision is a decision that in no stage of processing includes any human intervention.[63] As a consequence, it is not very likely that someone will be subjected to an automated decision, since it will almost always involve at least a tiny amount of human intervention. For example, in behavioural marketing campaigns, data concerning personality traits and browsing habits of individuals is collected and automatically segmented into predetermined market segments. The

[58] In the amended text of the European Parliament both aspects are joined in the same section of the article on the right of access, namely Article 15(2)(a).

[59] Swire / Lagos, (2013), 339.

[60] Lynskey (2015), 263.

[61] European Data Protection Supervisor (2015), 13.

[62] Irion / Luchetta, (2013), 68.

[63] Profiling that the article explicitly mentions can be therefore seen as an redundant. However, the legislature's point was probably to make sure that even when profiling is not fully automated the article applies.

question remains whether the act of determining the qualities of each market segment is sufficient to mean that this is not a fully automated system.[64] Such strict interpretation could dangerously narrow down the scope of the right, which could otherwise be a remedy for the challenges in the era of artificial intelligence,[65] where the automated decision-making has become the *modus operandi*.

Fully automated decisions are prohibited if they significantly affect an individual. Here as well, the meaning of "significantly affect" is open. Decisions in relation to employment certainly fall within this group, but the scope could be much wider. For instance, Borgesius suggests that even price discrimination that occurs as a consequence of Internet marketing could be subsumed under Article 22.[66]

3 Controlling Personal Data in the Big Data Era

Data has been at the heart of the shift from industry-based to information-based economies.[67] Its transformation into a highly valuable asset has created numerous business opportunities in the public and the private sector.[68,69] Some believe that data-enabled technological developments—social media, digital devices, artificial intelligence, robots and the Internet of Things—have been so significant that they have opened the way to the next technological revolution and laid the basis for Industry 4.0.[70] As Klaus Schwab, the founder and Executive Chairman of the World Economic Forum, puts it: "a fusion of technologies that is blurring the lines between the physical, digital and biological spheres has characterized a fourth industrial revolution".[71]

In the literature, these changes have often been associated with the emergence of the *big data revolution*.[72] In spite of its buzzword status and wide usage in a variety of contexts, big data still has no well-established definition. Most often, it is characterised by the *variety* of sources of data, the *velocity* at which they are collected and stored and their sheer *volume*, in what is commonly known as the "3-V definition".[73] However, nailing down the right definition is not the key point. What reveals the true

[64] Levin (2012), 139.

[65] See for example Edwards / Vaele (2017), 4.

[66] Borgesius (2015), 2.

[67] Davison (2003), 1.

[68] This also explains why, back in the eighties, data ownership set off a heated debate on the additional legislative protection of investment in the creation and marketing of database. Davison (2003), 52.

[69] See for example Organisation for Economic Cooperation and Development (2015), 23.

[70] Helbing (2014), 1.

[71] Schwab (2016).

[72] Mayer-Schonberger / Cukier (2013).

[73] Moerel (2014), 8.

power of big data and should be the focus of the discussion is its predictive power.[74] Big data analytics has the potential to foresee future trends and reveal patterns of individual behaviour that were previously impossible to spot. In line with this, ENISA's definition shifts the focus to the analytics phase and defines big data as "the technologies, the set of tools, the data and the analytics used in processing large amount[s] of data."[75]

Not only did the emergence of data-driven business models and ubiquitous algorithmic decision-making alter the rules of the game for businesses, it also significantly affected consumers. This is not surprising given that personal data proved to be a highly valuable source of business across different sectors.[76] Nowadays, more data are created about individuals than by individuals, and the multiplying character of Internet data means that even if data are removed at the source, copies can still be retained in caches (technical measures to foster efficiency on the net) or on mirror websites.[77] In the future, more and more personal data will be generated and will continue to exist under the control of others.[78] In Purtova's words, the notions of economic value and ownership of personal data have become routine in the realities of data processing practices and data protection and information systems scholarship.[79]

This highly complex data processing and the transformative use of personal information drastically limit the awareness of consumers, their capability to evaluate the various consequences of their choices, to give free and informed consent[80] and to exercise their control rights. For an ordinary citizen, coming into contact with the "big" data controllers is nearly impossible. Information symmetry and digital illiteracy exacerbate the problem. Therefore, it is not surprising that many authors have expressed concerns that data subject rights are being diluted and have proposed changes to the law.[81]

Calling for more data subject control seems to have become a mantra for the European policy,[82] but the approach that the regulators took to tackle the problems is not very promising. While EU policy makers seem to be devoted to the idea of empowered individuals and strengthened individual rights, they keep on using instruments that have proved useless in the past. This is obvious in relation to data subject rights. The paradox is nicely elaborated by Koops, who points out the discrepancy between the analysis of the problem (basically, the fact that users have no control over personal data in the world of big data) and the envisioned solution

[74] <https://www.privacyinternational.org/node/8>.

[75] ENISA (2015), 6.

[76] See for example Rubinstein (2012), 3.

[77] Koops (2011), 10.

[78] Executive office of the President (2014), 9.

[79] Purtova (2013), 4.

[80] Mantelero (2014), 643.

[81] See for example van der Sloot et al. (2016), 177; Koops (2014), 3.

[82] Lazaro / Le Métayer, (2015), 16.

(basically, to give users the rights and means to control their personal data in the world of big data).[83]

The following sections explore two sets of problems in relation to exercising control through data subjects' rights. The first set refers to the architecture of control rights, which makes them highly theoretical and often useless. The second relates to the question of controlling the data that is not personal but may nevertheless influence an individual.

3.1 Too Theoretical and Unworkable?

Due to technological developments the exercising of data subject rights has become highly theoretical. Koops writes: "Yes, you can be informed, if you know where to look and how to read (but who knows, looks, and reads?). Yes, you can request controllers to let you know what data they process, if you know that you have such a right in the first place (but which controller really understands and seriously complies with all such requests, particularly if exercised on an above-incidental scale?). Yes, you can request correction or erasure, if you know whom to ask (but how are you ever going to reach everyone in the chain, or mosaic, or swamp, of interconnected data processing?). There are simply too many ifs and buts to make data subject rights meaningful in practice."[84]

How challenging it can be to exercise the *right to information* and *the right of access* is well illustrated by the story of the former Austrian student Max Schrems. After studying in the US and learning about Facebook's data processing practices, Max Schrems decided to request his personal information kept by Facebook. Based on the EU Directive on Personal Data Protection, he invoked the right of access to personal data. In response Facebook sent him a file of 1200 pages, detailing all ways in which his personal data is deployed, shared and stored.[85]

The reason for the overwhelming amount of personal data processed by Facebook's was the company's highly complex business model. Facebook silently collects and stores an unimaginable amount of information including some very highly detailed data, e.g., recent donation to charity, brand of car someone drives as well as its age, and information about someone's household composition and ownership.[86] In addition to data coming from the tracks of a user's on-site activity, such as the pages he likes and the ads he clicks, Facebook's web-tracking efforts and its collaborations with major data brokers represent another significant source of data. By combining and mining these aggregated data, Facebook is able to derive rich personal profiles that reveal more than a user has intended to.

[83] Koops (2011), 22.

[84] Koops (2014), 4.

[85] <https://en.wikipedia.org/wiki/Max_Schrems>.

[86] Dewey (2016).

Today Facebook enables a more user-friendly experience. Within the Settings function a user can easily and speedily download her data. Contrary to Schrems' experience, this electronic copy of users' data is rather scant. For example, the history of a user's messages is presented in an incomplete and slightly chaotic way.

Moerel and Prins contend that the right of access is: "a paper tiger, and is certainly archaic when compared to the sophisticated ways in which the controllers are able to collect and process the data."[87] Indeed, navigating a 1200-page file can be very challenging even for a law student, let alone a layperson. In the wake of the Internet of Things, which encompasses the idea of ubiquitous data collection via sensors, exercising the right of access seems to become even harder if not impossible.[88]

Besides facilitating the inspection of the file, the right of access also guarantees access to information about the logic behind the automatic processing of information.[89] In other words, the law mandates that controllers provide information about the algorithms that are used to mine the data and discern patterns.[90] These algorithms are hard to audit, challenge or amend, and often characterised as black-box processes.[91] Take the example of Airbnb, an online peer-to-peer network that enables people to list, find, then rent vacation homes for a processing fee. How can a user know on what basis his property is rated and in what way he is connected to hosts? The information that the platform provides by default is very meagre. Tene and Polonetsky stress that in such cases businesses should at least be required to reveal the criteria used in their decisions, i.e. the outcome of the algorithmic calculation, if not the algorithms themselves.[92] Hildebrandt notes that Article 13(1)(f) actually provides more protection than the minimum sketched by Tene and Polonetsky. Next to an obligation to provide information about the existence of profiling and the criteria used, Article 13(1)(f) also requires that data subjects be informed about the envisaged consequences.[93] However, this is easier said than done. Goodman and Flaxman point out that algorithms are by nature hard to explain. It is questionable in which ways these information can be conveyed to users. "Putting aside any barriers arising from technical fluency, and also ignoring the importance of training the model, it stands to reason that an algorithm can only be explained if the trained model can be articulated and understood by a human."[94] Without doubt, fulfilling the Article 13 requirement in the big data era will be very

[87] Moerel / Prins, (2016), 65.

[88] Edwards (2016), 3.

[89] See page 8.

[90] Van der Slot et al. (2016), 146.

[91] See for example Pasquale (2015).

[92] Save for the algorithms that may be subject to protection of trade secrets and other intellectual property rights; Tene / Polonetsky, (2013), 9.

[93] Hildebrandt (2012), 51.

[94] Goodman / Flaxman, (2016), 6.

challenging, not least because, with less than 2 years until the GDPR takes effect, the clock is ticking.[95]

The *right to be forgotten* is another control right that may be challenged by big data developments. The socio-technical context of big data implies that data processing is based on vague purpose definitions to allow unforeseen future uses and that data are increasingly used for secondary purposes.[96] For example, in an increasingly personalised Internet almost every bit of personal data can be argued to be relevant[97] and it will be hard to establish that the data should be forgotten on the ground of "no longer being necessary for the purpose for which it was initially collected" (Article 17(1)(a)).

As of August 2017 the number of URLs that Google had evaluated for a removal under the right to be forgotten had climbed to 1.854.119.[98] However, the effectiveness of the right is disputable: researchers have found that deleted URLs in 30–40% of cases can still be identified.[99] Furthermore, Google and the French DPA are still fighting over the removal of links from Google's global domain.[100] For the time being, Google only deletes data from the European domains, which means that the data may still be accessible via the US one.[101]

The Twitter example offers another illustration of why the right to be deleted is flawed. Twitter's standard terms and conditions urge the users of Twitter's APIs[102] to cease processing and delete the tweets that have been removed by original posters. In reality, a tweet that has been removed from the user's timeline often continues to be processed on third parties' servers.[103] As mentioned above, under the GDPR Twitter as a controller only has an obligation to inform third parties about the erasure request but bears no further accountability. Due to inactive national data protection authorities and Twitter's scarce supervision as well as trivial penalties, deleting tweets from third parties' databases is unlikely to happen.[104]

Finally, the *right to data portability* remains a highly controversial issue, mainly because it is not clear from the legislative proposal whether this is a *'lex social network'* or concerns every other context, such as electricity providers and banks. According to the GDPR's recitals, the idea of data portability was introduced due to alleged lock-ins involving social networks.[105] However, it could be argued that its

[95] Goodman / Flaxman, (2016), 7.

[96] Koops, (2011), 16.

[97] Graux / Ausloos / Valcke, (2012), 13.

[98] < https://transparencyreport.google.com/eu-privacy/overview >.

[99] Xue / Magno / Cunha / Almeida / Ross, (2016), 13.

[100] The case is currently pending at the highest court of France; Robinson (2016).

[101] Gibbs / agencies (2016).

[102] An API (application programming interface) is a set of subroutine definitions, protocols, and tools for building software and applications.

[103] Ursic et al. (2016), 25.

[104] Ursic (2016), 7.

[105] While social networking sites like Facebook and Google+ offer users the possibility to obtain a copy of their data, there are still considerable limits on the direct transfer of personal information

definition should not be limited to one specific market, given the open definition in Article 18. Thus, open terms could make the provision applicable generally to all types of electronic processing including cloud computing, web services, smartphone apps and other automated data processing systems. Furthermore, lack of suitable standards and formats could mean that the right may be very difficult to implement. Unless transfer of data is smooth and requires no special technical knowledge, data portability could hardly contribute to strengthening data subjects' control. What is needed is more than mere portability. In particular, interoperability of the services between which the data is transferred is critical to the effectiveness of the right.[106]

3.2 Controlling Anonymous Data

The big data phenomenon also raises the issue of control over data that cannot be included in the category of "personal data".

Big data analytics typically tends to revolve around large quantities of aggregated data.[107] Typically, this data is anonymised, which means that it no longer allows identification of the individual to whom data used to relate, either directly or indirectly. Anonymised data is deemed non-personal data. Consequently, in these cases data protection law and corresponding control rights do not apply. However, even without identifying single individuals, aggregated data makes it possible to identify patterns in the behaviours of groups and these results can be used by data gatherers in order to construct profiles on which they base future decisions.[108] In this way the anonymised data that falls outside the scope of the data protection law can nevertheless influence an individual. Not only does such processing affect privacy—anonymised data can also put at risk other fundamental rights such as liberty and autonomy.[109] Hildebrandt contends that anonymised data may have the biggest impact on a person: "If three or four data points of a specific person match inferred data (a profile), which need not be personal data and thus fall outside the scope of data protection legislation, she may not get the job she wants, her insurance premium may go up, law enforcement may decide to start checking her email or she may not gain access to the education of her choosing."[110]

---

to other platforms. Moreover, social network providers do not allow third-party sites to directly acquire the user's information. For instance, Facebook blocks Google Chrome's extension for exporting friends. Graef et al. (2013), 6.

[106] This is not to say that interoperability comes with no disadvantages. For possible negative impacts, see Swire / Lagos, (2013), 356.

[107] Van der Sloot et al. (2016), 189.

[108] Mantelero (2014), 654.

[109] Custers (2004), 140.

[110] Hildebrandt (2013), 12.

Using anonymised data is typical of the behavioural advertising industry. Those companies are not interested in a user's actual identity, they simply wish to find consumers who are more likely than the average consumer to view their advertisement. The lack of human input, argues Lynskey, as well as the anonymous nature of the profiling and targeting exercise, makes it difficult to classify the behavioural advertising process as a type of individual surveillance.[111] Yet the perceived surveillance, occurring behind the scenes, can be equally damaging for an individual's privacy and can, among other things, cause a chilling effect.

In this anonymised environment control rights have lost their mission and new solutions will have to be found. One possibility is enhanced engagement of public authorities. Discussing the traps of data commodification, Corien Prins calls for "a debate on the role of the public domain in providing the necessary instruments that will allow us to know and to control how our behavior, interests and social and cultural identities are 'created'."[112] In a similar sense Mantelero claims that in the era of big data "the focus cannot be maintained mainly on the user and his or her self-determination: the role played by users should be restricted and conversely the role of independent authorities should be increased."[113]

4 Discussing Solutions

As shown above, traditional control rights have failed to function properly in the big data era. Data subject rights have been limited and trapped in a highly complex online labyrinth. Having realised the big data problem, many authors argue that it is critical to breathe some new life into data protection.[114]

One such alternative is the holistic approach, suggesting that an interplay of instruments from different fields could make data protection law better equipped for the challenges of the big data era. It is interesting to note that the GDPR incorporates a few solutions which all strongly resemble the ideas of the holistic approach. The most striking examples of the interplay between legal disciplines are provisions on data portability, the right to be forgotten and the right to information found in Chapter 2. The following section builds upon those pioneer steps and explains how the holistic approach could act as a measure to keep up with technological developments.

[111] Lynskey (2015), 216.

[112] Quoted in Lazaro / Le Métayer, (2015), 31.

[113] Mantelero (2014), 653.

[114] See for example van der Sloot et al. (2016), 177; Koops (2014), Thierer (2013), 411.

4.1 Strengthening the Right to Information Through the Features of Consumer Protection Law

The section on data subject rights begins with an article on transparency of information, communication and modalities for the exercise of the right of the data subject (Article 12 of the GDPR). At the outset, the article requires a controller to provide this information *"in a concise, transparent, intelligible and easily accessible form, using clear and plain language"*. The transparency requirement was not part of the DPD; it was only briefly mentioned in the recitals, which did not constitute the binding text.

The wording of the new Regulation echoes typical consumer protection clauses by stressing the importance of transparency and intelligibility. For example, Article 7 of the Directive on consumer rights[115] uses almost identical wording as Article 12: "*information shall be legible and in plain, intelligible language*." The nudging approach is further reflected in the extensive list of information that a controller needs to communicate to an interested data subject, in the shifted burden of proof and in the possibility to provide the information in the form of standardised icons. The visualisation of privacy policies (Recital 58), which are often too complex for an average reader to comprehend, is a helpful, yet another paternalistic measure. While it is common to stumble across such provisions in consumer protection laws, they are less typical for data protection statutes.

One of the main concerns for the European consumer law has been to provide consumers with all the information they need to make informed choices. According to Articles 5(1)(c) and 6(1)(e) of the Directive on consumer rights, the trader shall provide the consumer with the information on *"the total price of the goods or services inclusive of taxes.*" Similarly, Articles 6 and 7 of the Directive on Unfair Commercial Practices[116] stress the prominent position of information as a prerequirement for fair business-to-consumer contracting.[117] Because consumer protection law in principle applies to contracts that are based on money exchange, it has been rarely brought up in the debate on terms imposed by online social service providers. Namely, these services typically use the freemium pricing strategy, which is not based on money but on personal data exchange and thus in principle falls outside the scope of consumer protection law.

Arguably, this is bound to change. The European Commission's proposal for a Directive on certain aspects concerning contracts for the supply of digital content has acknowledged the urge for modifications. The Directive represents the first legal act in which "paying with personal data" is recognised as a counter-performance in

[115] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, [2011] OJ L 304.

[116] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market, [2005] OJ L 149.

[117] Helberger (2016), 9.

business-to-consumer contracting.[118] As the Commission explains in the recitals: "In the digital economy, information about individuals is often and increasingly seen by market participants as having a value comparable to money. Digital content is often supplied not in exchange for a price but against counter-performance other than money i.e. by giving access to personal data or other data. [… D]efects of the performance features of the digital content supplied against counter-performance other than money may have an impact on the economic interests of consumers."[119] In other words, consumer protection safeguards should also apply to contracts where consumers actively provide counter-performance other than money in the form of personal data or any other data.

Profiling and targeting strategies driven by the Internet of Things can amount to significantly impairing a consumer's freedom of choice or conduct. The actual impact depends on the persuasive potential of the personalised message and the extent to which the practice reduces the autonomous decision making process.[120] The Unfair Commercial Practices Directive could be used to mitigate negative impacts and help consumers. Helberger suggests that where the data is being used not only to provide the service but also to extract extra commercial value from that data, and doing so without telling the consumer, it could constitute an unfair commercial practice under 5(2) of the Directive concerning unfair business-to-consumer commercial practices in the internal market.[121] The EU Directive on unfair terms could work to achieve the same aim. The Directive defines as unfair a term that, contrary to the requirement of good faith, causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer.[122] How this provision could protect individuals sharing their data on the Internet can be explained through the example of an agreement between a mobile phone user and an app developer. In this contract the app developer grants the consumer a licence to use an app in return for which the consumer allows the developer, acting as a data controller, to collect location and usage data to provide advertising for as long as the app is installed.[123] While this exchange of consumer data for a

[118] Article 3(1) of the proposed Directive gives exchange with data the same status as money*: "This Directive shall apply to any contract where the supplier supplies digital content to the consumer or undertakes to do so and, in exchange, a price is to be paid or the consumer actively provides counter-performance other than money in the form of personal data or any other data."*

[119] Recital 13 of the proposal for a Directive on certain aspects concerning contracts for the supply of digital content, COM(2015) 634 final, 9.12.2015.

[120] Helberger gives an example of a consumer who is being targeted with diet products after she has learned from her scale that she has gained a couple of kilos. To assert unfair practice under the Directive it would be necessary to better understand how deep the fear of gaining extra weight is (is she obese or bulimic, over- or normal weight, what is her age, does she have a history of (unsuccessful) dieting, etc.), how receptive the user is to personalisation strategies, how much the timing of the message plays a role etc. Helberger (2016), 20.

[121] Helberger (2016), 10.

[122] Article 3 of Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, [1993] OC L 095.

[123] Rhoen (2016), 7.

licence can be legal under data protection law (the data subject has given his or her consent), it is not necessarily so under consumer protection law. Rhoen argues that such a case "would almost certainly violate [… the Unfair Terms Directive]. Allowing surveillance in exchange for the ability to switch an LED on or off seems like such a bad deal, that the "requirement of good faith" has probably not been met."[124]

4.2 From Portability to Prosumer Law

Data portability is not a standard component of data protection statutes. It is striking that it actually represents an anti-trust measure. Personal data portability can be compared to the number portability in the EU telecommunications law, which was introduced in 2002 as part of the Universal Service Directive[125] to help mobile phone users change telecommunication providers.[126] However, in contrast to number portability, which was imposed in order to facilitate consumer choice and effective competition in the telecommunication market, data portability has an extra objective, namely, protection of personal data and privacy, which explains why the GDPR drafters insisted on its insertion in the data protection code.

Admittedly, data portability could have numerous positive implications for data subjects. First, in some markets, such as social networks, data portability may significantly lower switching costs for users. Second, promoting markets for privacy through data portability could be a promising strategy to help privacy attributes become more salient in competition.[127] Finally, allowing data portability could let individuals benefit from the value created by the use of their personal data: they could license the data for further use to third parties, in exchange for additional services, or for cash value.[128] With the recent technology advances, personal data has also become a means of self-expression (see the "quantified self" movement),

[124] Ibid.

[125] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services, [2002] OC L 108.

[126] Ibid., Article 30: *"Number portability.*

1. Member States shall ensure that all subscribers of publicly available telephone services, including mobile services, who so request can retain their number(s) independently of the undertaking providing the service:

(a) in the case of geographic numbers, at a specific location; and

(b) in the case of non-geographic numbers, at any location.

This paragraph does not apply to the porting of numbers between networks providing services at a fixed location and mobile networks.".

[127] Irion / Luchetta, (2013), 42.

[128] European Data Protection Supervisor (2015), 13.

which suggests that portability could play an important role in safeguarding one's own (representation of) identity in personal data.[129]

However, some authors stress that antitrust is ill equipped to solve consumer law and privacy problems. Harm to privacy does not per se equal harm to competition (and vice versa). Applying data portability to all data controllers, be it the world's largest corporation or a start-up, without examining the relevant market and competitors' positions in more detail, could lead to distortion of competition.[130] For the same reasons several EU Member States in the Council opposed the proposal for data portability and expressed the view that portability is rather a tool to enhance competition and therefore falls outside the ambit of data protection legislation.[131]

While these concerns are indeed worth further consideration, the academic mainstream seems to be in favour of data portability as a measure at the crossroads between antitrust and data protection.[132] For example, Brown and Marsden see data portability as an inherent part of what they call prosumer law, which they describe as a legal instrument that is urgently needed to enable European citizens to make most effective use of the opportunities offered in the data-driven economy. Through the lens of prosumer law a modern Internet user is both consumer and producer of content (data in all forms). This suggests a more targeted intervention to prevent social networks from erecting a fence around their piece of the information commons. However, this can be only ensured if portability is supported by interoperability with open standards.[133] Combining these two measures would enable prosumers to effect a meaningful exit, control their own prosumption, or continue their personal data capture.[134]

It is expected that the interplay of data protection and competition law for the purpose of strengthening protection of individuals will intensify in the future. Lynskey predicts an increased debate in the EU regarding the potential connections between data protection and competition law that would go beyond data portability.[135] The European Data Protection Supervisor has made clear that privacy harms reduce consumer welfare; as the latter is a principal goal of the modern competition law, data protection objectives should necessarily be addressed in an antitrust analysis.[136] In the past, the practice of the EU Directorate General for Competition showed no special affection for this idea[137] but, as Lynskey contends, in the big data era this might change.

---

[129] Rhoen (2016), 9.

[130] Swire / Lagos, (2013), 339.

[131] Graef et al. (2015), 9.

[132] Graef (2013), 512.

[133] Brown / Marsden, (2013), 25.

[134] Brown / Marsden, (2013), 28.

[135] Lynskey (2015), 265.

[136] European Data Protection Supervisor (2014), 2, 16.

[137] See for example European Commission, COMP/M.4731 - Google/DoubleClick; European Commission, COMP/ M.4854 – TomTom/TeleAtlas.

4.3 Control Rights in Personal Data as a Replication of the Author's Moral Right

Rights that not only affect the contracting party (*omnes partes*) but also extend to third parties (*erga omnes*) are a typical characteristic of the property law regime.[138] The right to be forgotten as an entitlement to block all further, secondary uses somewhat resembles such *erga omnes* provisions.

In the 2012 version of the GDPR proposal, Article 17(1) explicitly allowed data subjects to seek the deletion of data and block further reuse when consent is withdrawn or when the data is no longer necessary in relation to the purposes for which it was collected or otherwise processed. Furthermore, Article 17(2) proposed that the right to be forgotten should follow the data when the data controller has made it public (e.g., by publishing it on a website) or when publication is delegated to a third party. In the first scenario, the original controller only has to take 'all reasonable steps' to inform third parties about the data subject's request for erasure. In the second situation, the original controller will be considered responsible in any case.

The wording of Article 17(2) has the capacity to radically shift the burden of proof—it is for the data controller and not for the individual to prove that the data cannot be deleted because it is still needed or relevant.[139] Exercising the right to be forgotten would then mean influencing third parties, i.e. generating *erga omnes* effects.

Article 17(2) was probably what made Kuner state that the GDPR proposal was a Copernican shift in the EU data protection law.[140] Unfortunately, the provision was later left out of the GDPR due to intense opposition from lobbying groups representing controllers.[141] Without doubt, the level of individual protection was considerably decreased as a result of the amendment.

Although personal data protection is interpreted as part of privacy, which is a human right, it is impossible to deny that the big data economy treats personal data as an asset.[142] While some may be critical of the idea of perceiving personal data as a commodity, others believe that merging data protection law with certain features of the property rights regime could in fact strengthen privacy protection.[143] Purtova contends that as long as personal data bears high economic value "the real question is not 'if there should be property rights in personal data', but 'whose they should be'".[144]

Two conclusions stem from the debate on property and data protection control rights. First, the Regulation's scheme can be compared to the distinct area of

[138] Victor (2013), 519.

[139] European Commission (N.D.).

[140] Kuner (2012), 1.

[141] Fleming (2013).

[142] Victor (2013), 522.

[143] See for example Schwartz (2004), 2058.

[144] Purtova (2013), 28.

intellectual property: the moral rights of artists.[145] This is the part of intellectual property which grants an artist a proprietary interest in his own work, even after it has been sold, that prevents others from altering or destroying the work. While permitting the trading of intellectual assets, the law does not allow artists to give up certain rights such as recognition of authorship. Moral rights could be a good model of how to balance the fact that personal data is both—a commodity and an object protected as a fundamental value.

Second, instead of striving for individual ownership over personal data, an alternative to protect citizens' privacy could be a shift towards common data property. This form of data ownership can be achieved, for instance, through dedicated platforms, which would enable citizens to safely store, manage and share their data. Such platforms would be organised as co-operatives that are solely owned and controlled by their members and not by shareholders, thus eventually giving the members more control over data use and management.[146] The idea behind common data property is that the control exercised by a social group is more resilient than when it is exercised by an individual.

5 Implications for the Future Policy and for Those Who Will Interpret the New Law: Conclusions

The changing technological landscape in which personal data is processed presents a challenge for personal data protection. As shown above, in the big data era data protection law is often diluted and this holds true particularly for data subject rights. In addressing the issue the EU regulator mainly sticks to the traditional approach to control rights. However, the upcoming GDPR contains some novel solutions. Their common trait is that they resemble instruments from various legal domains such as consumer protection law, (intellectual) property law and competition law.

This policy approach implies the potential for a more holistic legal scheme in EU law in relation to personal data as well as the need for additional interfaces between data protection and other legal fields. As the GDPR will only enter into force in 2018, it may be too early to discuss the actual outcomes. Nevertheless, my thesis is that this new strategy could amount to a better balance between data subject rights and economic needs in the big data economy. If the instruments are combined smartly, and implemented with prudence and sufficient understanding of the specifics of each legal area, the holistic approach has the potential to heal some of the

[145] Victor (2013), 524.

[146] Hafen et al. (2014), 3; Also see Vayena / Gasser, (2016), 2: *"An individual's right to privacy is widely assumed to be antagonistic to the health-related public goods resulting from openness. In this view, an individual's right to privacy may have to be infringed upon to promote the public good. There is a legitimate public interest in genomic data, it is believed, justifying such infringements for the greater good. But this view of the relationship between the right to privacy and the public good of health is too crude."*.

long-lasting discrepancies in data protection law and strengthen data subject control rights.

However, not all the drawbacks of the big data economy can be healed by strengthening control rights. In cases when data is anonymised and decisions are taken at group level, neither more control rights nor a holistic approach can help. Rather, other solutions, e.g. intervention of data protection or consumer authorities, have to be found.

Obiter dictum, I want to briefly comment on control as a normative anchor of privacy law. In the light of big data it might be advisable to reconsider the underlying objectives of privacy and data protection, in particular the significance of someone's control over data as a normative objective. As Vayena and Gasser point out—privacy is not about maximal levels of controls, but rather about reasonable measures of control.[147] Indeed, both data protection and privacy laws are a balancing regulation striving for equilibrium between protection of data subjects and other legitimate goals.[148] However, at some points (e.g. Recital 7 of the GDPR) the regulator seems to exaggerate its mission to reinforce data subjects' control. There are two reasons why this is not the right way to go. First, striving for absolute control is unpractical and unrealistic, and second, in certain cases, e.g. in genomics research, excessive data subject control can be an obstacle to innovation and science prosperity. Viewed through the lens of the holistic approach to data protection, this is an essential finding. The acknowledgment that individual control in the genuine data protection sense is not and should not be a means to the end may enhance the interplay between legal disciplines in their mission to better protect individuals, while allowing innovation and economy to flourish.

References

Borgesius, J.Z.F. (2015), Online price discrimination and data protection law, Amsterdam Law School Legal Studies Research Paper No. 2015-32

Brown, I. / Marsden, C.T. (2013), Regulating Code-Towards Prosumer Law, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2224263

Burton, C. / De Boel, L. / Kuner, C. / Pateraki, A. / Cadiot, S.G. / Hoffman, S. (2016), The Final European Union General Data Protection Regulation, Privacy & Security Law Report 2016, 15

Custers, B. (2004), The power of knowledge: ethical, legal and technological aspects of data mining and group profiling in epidemiology, Wolf Legal Publishers

Custers, B. (2013), Data Dilemmas in the Information Society: Introduction and Overview, in: B. Custers / T. Calders / B. Schermer / B. Zarsky (Eds.), Discrimination and Privacy in the Information Society – Data Mining and Profiling in Large databases, Springer

Custers, B. / van der Hof, S. / Schermer, B. (2014), Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies, Policy & Internet 2014, 3

[147] Vayena / Gasser, (2016), 3.

[148] EU Court of Justice, Google Spain v. AEPD and Mario Costeja Gonzalez, C-131/1, ECLI:EU:C:2014:317; Charter of Fundamental Rights of the European Union, Article 8 (2); Article 9(2) of the GDPR etc.

Crawford, K. / Schultz, J. (2014), Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms, B.C.L. Rev. 2014, 93

Davison, M.J. (2003), The legal protection of databases, Cambridge University Press

Dewey, C. (2016), 98 personal data points that Facebook uses to target ads to you, the Washington Post of 19 August 2016, available at: https://www.washingtonpost.com/news/the-intersect/wp/2016/08/19/98-personal-data-points-that-facebook-uses-to-target-ads-to-you/?tid=sm_tw&utm_term=.2ceafb44a4d3

Edwards, L. (2016), Privacy, security and data protection in smart cities: a critical EU law perspective, European Data Protection Law Review 2016, 1

Edwards, L. / Vaele, M. (2017), Slave to the Algorithm? Why a 'Right to Explanation' is Probably Not the Remedy You are Looking for, available at: https://poseidon01.ssrn.com/delivery.php?ID=608092126118023018120070086020112094059092037020027043122087105090122106076117000118007114061061050022034101117002121010092102023006066082083003119085105108077067096010048051118102123095086028105074026123084120073122028102120108029012011082084065119013&EXT=pdf

ENISA (2015), Big Data Security - Good Practices and Recommendations on the Security of Big Data Systems, available at: https://www.enisa.europa.eu/publications/big-data-security/at_download/fullReport

European Commission (2010), Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee Of the Regions; A comprehensive approach on personal data protection in the European Union, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52007DC0575

European Commission (N.D.), Factsheet on the "Right to be Forgotten ruling" (C-131/12), available at: http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf

European Data Protection Supervisor (2014), Preliminary Opinion of the European Data Protection Supervisor - Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf

European Data Protection Supervisor (2015), Opinion 7/2015 - Meeting the challenges of big data - A call for transparency, user control, data protection by design and accountability, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf

Executive Office of the President (2014), Big Data: Seizing Opportunities, Preserving Values, available at: https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf

Federal Trade Commission (1998), Privacy Online: A Report to Congress, available at: https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf

Fleming, J. (2013), New data protection rules at risk, EU watchdog warns, EuroActiv.com of 30 May, available at: http://www.euractiv.com/section/digital/news/new-data-protection-rules-at-risk-eu-watchdog-warns/

Gibbs, S. / agencies (2016), Google to extend 'right to be forgotten' to all its domains accessed in EU, The Guardian of 11 February 2016, available at: https://www.theguardian.com/technology/2016/feb/11/google-extend-right-to-be-forgotten-googlecom

González Fuster, G. (2014), The Emergence of Personal Data Protection as a Fundamental Right of the EU, Springer International Publishing

Goodman, B. / Flaxman, S. (2016), European Union regulations on algorithmic decision-making and a "right to explanation", available at: https://arxiv.org/pdf/1606.08813.pdf

Graef, I. (2013), Mandating portability and interoperability in online social networks: regulatory and competition law issues in the European Union, Telecommunications Policy 2015, 6

Graef, I. / Verschakelen, J. / Valcke, P. (2013), Putting the Right to Data Portability into a Competition Law Perspective, The Journal of the Higher School of Economics, Annual Review

Graux, H. / Ausloos, J. / Valcke, P. (2012), The Right to be Forgotten in the Internet Era, ICRI Research Paper No. 2012, 11

Hafen, E. / Kossmann, D. / Brand, A. (2014), Health Data Cooperatives – Citizen Empowerment, Methods of Information in Medicine 2014, 2

Helberger, N. (2016), Profiling and targeting consumers in the IoT, available at: http://www.ivir.nl/publicaties/download/1747.pdf

Helbing, D. (2014), Economy 4.0 and Digital Society: The Participatory Society is Born (Chapter 8 of Digital Economy), available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2539330

Hijmans, H. (2016), The European Union as a constitutional guardian of internet privacy and data protection, University of Amsterdam, available at: https://pure.uva.nl/ws/files/2676807/169421_DEFINITIEF_ZELF_AANGEPAST_full_text_.pdf

Hildebrandt, M. (2012), The Dawn of a Critical Transparency Right for the Profiling Era, Digital Enlightenment Yearbook 2012, IOS Press

Hildebrandt, M. (2013), Slaves to Big Data. Or Are We? IDP Revista De Internet, Derecho Y Política 2013, 16

Irion, K. / Luchetta, G. (2013), Online Personal Data Processing and the EU Data Protection Reform, Centre for European Policy Studies, 2013, available at: http://www.ceps.eu/book/online-personal-data-processing-and-eu- data-protection-reform

Jackson, H. (2012), Chapter 8 – Information Provision Obligations, in: E. Ustaran (Ed.), European privacy: law and practice for data protection professionals, International Association of Privacy Professionals (IAPP)

Kokott, J. / Sobotta, C. (2013), The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, International Data Privacy Law 2013, 4

Koops, B.-J. (2011), Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice, SCRIPTed 2011, 3

Koops, B.-J. (2014), The trouble with European data protection law, International Data Privacy Law 2014, 4

Koops, B.-J. / Newell, B.C. / Timan, T. / Škorvánek, I. / Chokrevski, T. / Galič, M. (2016), A Typology of Privacy, University of Pennsylvania Journal of International Law 2016, 2

Kroes, N. (2011), Online privacy – reinforcing trust and confidence, Speech/11/461, available at: http://europa.eu/rapid/press-release_SPEECH-11-461_en.htm

Kuner, C. (2012), The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law, Privacy & Security Law Report 2012, 6

Lazaro, C. / Le Métayer, D. (2015), Control over personal data: True remedy or fairytale? SCRIPTed 2012, 1

Levin, M. (2012), Chapter 9 – Data Subjects' Rights, in: E. Ustaran (Ed.), European privacy: law and practice for data protection professionals, International Association of Privacy Professionals (IAPP)

Lynskey, Orla (2014), Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order, International and Comparative Law Quarterly 2014, 3

Lynskey, O. (2015), The Foundations of EU Data Protection Law, Oxford University Press

Mantelero, A. (2014), The future of consumer data protection in the EU Re-thinking the "notice and consent" paradigm in the new era of predictive analytics, Computer Law & Security Review 2014, 6

Mayer-Schonberger, V. / Cukier, K. (2013), Big Data: A Revolution That Will Transform How We Live, Work and Think, John Murray Publishers

Meyer, D. (2016), Uber Just Made a Big Concession to Moscow's Transport Authorities, Fortune of 15 March 2016, available at: http://fortune.com/2016/03/15/uber-moscow-concession/

Moerel, E.M.L. (2014), Big data protection: How to make the draft EU Regulation on Data Protection Future Proof, Tilburg University, available at: https://pure.uvt.nl/portal/files/2837675/oratie_Lokke_Moerel.pdf

Moerel, L. / Prins, C. (2016), Privacy for the homo digitalis - Proposal for a new regulatory framework for data protection in the light of Big Data and the Internet of Things, available at: https://doi.org/10.2139/ssrn.2784123

Organisation for Economic Cooperation and Development (2015), Data-Driven Innovation - Big Data For Growth And Well-Being, available at: http://oe.cd/bigdata

Pasquale, F. (2015), The Black Box Society - The Secret Algorithms That Control Money and Information, Harvard University Press

Purtova, N. (2013), The Illusion of Personal Data as No One's Property, Law, Innovation, and Technology 2013, 1

Purtova, N. (2014), Default Entitlements in Personal Data in the Proposed Regulation: Informational Self-Determination Off the Table ... and Back on Again? Computer Law and Security Review 2014, 1

Rhoen, M. (2016), Beyond consent: improving data protection through consumer protection law. Internet Policy Review 2016, 1

Robinson, D. (2016), Google appeals Right to be Forgotten ruling by French data body, Finacial Times of 19 May 2016, available at: https://www.ft.com/content/db71f034-1dd3-11e6-b286-cddde55ca122

Rubinstein, I. (2012), Big Data-The End of Privacy or a New Beginning, NYU School of Law, Public Law Research Paper No. 12-56, available at: https://ssrn.com/abstract=2157659

Sartor, G. (2015), The right to be forgotten in the Draft Data Protection Regulation, International Data Privacy Law 2015, 1

Schwab, K. (2016), The Fourth Industrial Revolution: what it means, how to respond, World Economic Forum, 14 January 2016, available at: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

Schwartz, P. (2004), Property, privacy and personal data, Harvard Law Review 2004, 7

Solove, D.J. (2002), Conceptualizing Privacy, Cal. L. Rev. 2002, 1087

Solove, D.J. (2015), 10 Implications of the New EU General Data Protection Regulation, TeachPrivacy, 23 December 2015, available at: https://www.teachprivacy.com/new-eu-data-protection-regulation-gdpr/

Swire, P. / Lagos, Y. (2013), Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique, Md. L. Rev. 2013, 72

Tene, O., / Polonetsky, J. (2013), Judged by the Tin Man; Individual Rights in the Age of Big Data, Journal of Telecommunications and High Technology Law 2013, 11

Thierer, A.D. (2013), The Pursuit of Privacy in a World Where Information Control is Failing, Harvard Journal of Law & Public Policy 2013, 36

Ursic, H. / Custers, B. / Olmedo, M. (2016), WP2 Developing the initial model - D2.2 Report on the legal analysis, EuDEco - Modelling the European data economy, available at: https://www.universiteitleiden.nl/binaries/content/assets/rechtsgeleerdheid/metajuridica/d2.2_reportonthe-legalanalysis-v1_2016-02-29.pdf

Ursic, H. (2016), The Right to be Forgotten or the Duty to be Remembered? Twitter data reuse and implications for user privacy, Council for Big Data, Ethics, and Society, available at: http://bdes.datasociety.net/council-output/the-right-to-be-forgotten-or-the-duty-to-be-remembered-twitter-data-reuse-and-implications-for-user-privacy/

van der Sloot, B. / Broeders, D. / Schrijvers, E. (2016), Exploring the Boundaries of Big Data, Amsterdam University Press

van Hoboken, J. (2013), The Proposed Right to be Forgotten Seen from the Perspective of Our Right to Remember Freedom of Expression Safeguards in a Converging Information Environment, available at: http://www.law.nyu.edu/sites/default/files/upload_documents/VanHoboken_RightTo%20Be%20Forgotten_Manuscript_2013.pdf

Vayena, E. /Gasser, U. (2016), Between Privacy and Openess in Genomics, PLOS Medicine 2016, 1

Victor, J.M. (2013), The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy, Yale Law Journal 2014, 2

Werro, F. (2009), The Right to Inform v. the Right to be Forgotten: A Transatlantic Clash, in: C. G. AC Ciacchi / P. Rott / L.J. Smith (Eds.), Haftungsbereich im dritten Millennium / Liability in the Third Millennium, Nomos

Westin, A.F. (1970), Privacy and Freedom, Atheneum New York

Xue, M. / Magno, G. / Cunha, E. / Almeida, V. / Ross, K.W. (2016), The Right to be Forgotten in the Media: A Data-Driven Study, Proceedings on Privacy Enhancing Technologies 2016, 4

Yu, H. / Robinson, D.G. (2012), The new ambiguity of the open government, UCLA L. Rev. Disc. 2012, 178

Zanfir, G. (2012), The Right to Data Portability in the Context of the EU Data Protection Reform, International Data Privacy Law 2012, 2

The Ambivalence of Algorithms

Gauging the Legitimacy of Personalized Law

Philipp Hacker

Contents

1 Introduction 86
2 Digital Market Failures 88
3 The Promise of Personalized Law 92
4 The Legitimacy of Personalized Law 95
4.1 Challenges Posed by Positive Law 95
4.2 Equality and Justice 98
4.3 Challenges Posed by Legal and Democratic Theory 105
5 The Scope of Personalized Law: A Normative Approach 108
6 Conclusion 110
References 112

Abstract This chapter maps out the irreducible ambivalence inherent in algorithms, and particularly Big Data techniques, that become evident when confronted by the law. This ambivalence, and its legal consequences, are explained in four steps. The first part of the chapter deals with the darker sides of the digital economy: the use of behavioral algorithms by private companies in market settings not only drives one of the most innovative parts of the economy, but has also given rise to what may be called "digital market failures". Remedial strategies are complicated by widespread actor heterogeneity. Hence, traditional regulation not only risks lagging behind technological progress, but also being overly restrictive for some and overly permissive for others.

Against this backdrop, the chapter in a second step explores how personalized law can be used to mitigate digital market failure while simultaneously accommodating actor heterogeneity. Using Big Data techniques, personalized law promises to tailor legal norms, from disclosures to mandates, to the individual characteristics of

Philipp Hacker is an A.SK Fellow at WZB Berlin Social Science Center, and a Postdoctoral Fellow at Humboldt University of Berlin.

This chapter drafted in the fall of 2016.

P. Hacker (✉)
WZB Berlin Social Science Center, Berlin, Germany
e-mail: philipp.hacker@rewi.hu-berlin.de

M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law*, MPI Studies on Intellectual Property and Competition Law 28, https://doi.org/10.1007/978-3-662-57646-5_5

addressees. Unlike one-size-fits-all regulation, personalization respects actor heterogeneity by actively harnessing the potential of digital technology for social good. However, the use of individualized, potentially privacy-sensitive information (such as personality traits or degrees of rationality) by the regulator raises a host of concerns of its own.

Therefore, the third part of the chapter develops an account of challenges to the legitimacy of personalized law stemming from both positive law and legal theory. While most of these objections can be accommodated by specific design features of personalized law, the chapter nonetheless argues that it must be used with care and after rigorous scrutiny on a case-by-case basis. For example, its use might be most valuable precisely in the very instances of digital market failures discussed in the first part of the chapter.

Accordingly, the fourth part suggests a normative approach to personalized law, under which due weight is given to the interests of all concerned parties. A key result of the analysis is that, if used prudently, personalized law will, counterintuitively, strengthen legal equality by making the differential impact of legal norms on different actors legally relevant, thus avoiding the pitfall of treating fundamentally different situations in the same way. However, such a démarche must be accompanied by enhanced public scrutiny of algorithmic lawmaking. As more and more economic and regulatory processes become subject to the power of algorithms, the crucial challenge is to develop a robust democratic discourse so that algorithmic decision making is not treated as a hermetic black box, but is infused with and guided by those societal values on which a legally constituted market economy undoubtedly rests.

1 Introduction

In contemporary legal scholarship, Big Data is often perceived as a threat—to individual privacy,[1] to unmanipulated markets,[2] or to meaningful agency in a "scored society".[3] This chapter claims that such threat-driven appraisals of Big Data only capture half of the truth. While it is true that data-mining technologies harbor novel and unique challenges for a range of fields and concepts in law, they may also be actively harnessed by the regulator to advance public-good-oriented goals such as fairness, non-discrimination, or legal equality. Personalized law, which tailors legal norms to individual subjects using Big Data technology, is one key example for the potential beneficial impact of digital technology in regulation. In developing a legal framework for the digital economy, we should therefore bear in mind that algorithms, like any new technology, are inherently ambivalent—used by private actors,

[1] See, e.g., Tene / Polonetsky (2012).

[2] Calo (2014).

[3] See Pasquale (2015); Citron / Pasquale (2014).

they bring about regulatory challenges, but used by the regulator, they also hold the promise of new and more effective forms of regulating the marketplace.

This chapter aims to illustrate this ambivalence in four parts. First, it will shed some light on the key challenges posed by the use of data-mining technologies by private actors and companies in market interactions. As I argue, three distinctive yet interrelated problems have been created or exacerbated by the advent of digital technology in the marketplace: (1) an attitude-action gap of users vis-à-vis the collection and protection of their personal data, with user surveys highlighting a sense of loss of control which is not matched by an increase in the use of encryption or protection devices easily available in the digital market; (2) the potential for exploitative contracts resulting from what may be called "computation power asymmetry" between technologically-empowered sellers and technologically-disempowered buyers, explored in an increasing body of literature in experimental and theoretical economics; (3) and finally a growing threat of discrimination by the use of behavioral algorithms, highlighted in a nascent branch of the literature in computer science.

Different solutions, ranging from transparency[4] via a specific regulatory authority for algorithms[5] to mandated active choice,[6] have been proposed in the literature to tackle these three problems. This chapter, however, takes a different tack. It begins with a discussion of the novel regulatory technique of personalized law[7] with a view toward meeting the challenges described in the first part. The construction of personalized law proceeds in five steps. First, individuals have to be sorted along some metric, for example a category of cognitive psychology, with the help of Big Data. Second, specific norms can be tailored, in the abstract, to scores in these categories; for example, disclosures to consumers might be different depending on whether they are assumed to be present-biased or not. Third, an entity has to allocate the concrete personalized law to each individual, based on their individual scores. Fourth, the relevant scores must be stored and updated. Fifth, the concrete personalized regime applying to an individual must be communicated to the counterparty before a transaction takes place.

Generally, personalized law, if applied properly, can solve the problem of heterogeneity within the pool of regulated subjects. However, as this chapter goes on to argue, it is subject to three types of challenge that question its legitimacy. First, in positive law, severe constraints regarding the use of personal data by the regulator are imposed by data protection law. Second, it must meet basic requirements of legal equality and justice. Third, the concept of personalized law also fundamentally transforms the way laws traditionally have been thought to express social and even moral norms, and in doing so it necessitates novel forms of democratic discourse

[4] Pasquale (2015), Chapters 5 and 6; Citron / Pasquale (2014).

[5] Tutt (2016).

[6] Hacker / Petkova (2016).

[7] See Porat / Strahilevitz (2014); Ben-Shahar / Porat (2016); Hacker (2016a), 321-322.

about lawmaking. Against this backdrop, this chapter develops a critical assessment of the legitimacy of personalized law.

The final part brings together the different threads running through the previous sections. I argue that the thus far under-reflected negative implications of personalized law should caution against its wholesale use. Rather, it should be deployed in very specific instances in which its expected benefits clearly exceed its expected costs, including privacy concerns, equality and justice considerations, and potential losses of democratic oversight. Hence, we need a balanced and normative approach. If these drawbacks are adequately addressed, personalized law in specific instances can be used to beat companies, and other actors, using unacceptable forms of data mining at their own game, i.e., with the help of digital technology. Thus, the ambivalence of algorithms can be productively used for social good.

The remainder of the chapter proceeds as follows: Sect. 2 describes various digital market failures. Section 3 explains how personalized law works and what its potential benefits are. Section 4 explores challenges to the legitimacy of personalized law. Section 5 argues for a specific scope of personalized law under a normative approach. Section 6 concludes.

2 Digital Market Failures

Digitization is not only rapidly transforming the way we interact with the everyday world around us, but also the way in which companies, and their clients, behave in markets. In this chapter, I focus on the most pervasive digital technology driving innovation at the moment: Big Data. Analytics drawing on Big Data generated estimated worldwide revenues of $122 billion in 2015, and this amount is projected to increase by more than 50% in the next 5 years.[8] While a definition of Big Data with universal currency has not yet emerged in the literature,[9] it involves the computer-based collection and processing of data sets that are particularly large,[10] varied,[11] or unstructured.[12] Broadly speaking, Big Data analytics are thus used to discover structures, correlations, and regularities in specific data sets that could not be fruitfully analyzed before the advent of computational algorithms. Algorithms, in turn, are well-defined instructions, often in machine-readable format, which tell a computer how to generate an output from a given input.[13]

[8] IDC, Press Release, Worldwide Big Data and Business Analytics Revenues Forecast to Reach $187 Billion in 2019, According to IDC, 23 May 2016.

[9] Gandomi / Haider (2015), 138.

[10] Colonna (2013), 329.

[11] Gandomi / Haider (2015), 138.

[12] Gandomi / Haider (2015), 137.

[13] Cormen / Leiserson / Rivest / Stein (2009), 5.

The rise of the algorithm,[14] and more broadly of the digital economy,[15] is driving innovation at a pace that reminds some scholars of the Industrial Revolution.[16] Indeed, most of the gadgets many of us cherish would be unimaginable without algorithmic processing of information. However, the unilateral use of Big Data analytics by companies in market settings, and particularly the employment of predictive analytics aimed at forecasting the future behavior of data subjects,[17] also creates what I here call "digital market failures". In the next paragraphs, I briefly review what I believe are three of the most challenging instances of digital market failure[18]: the privacy "attitude action gap"; exploitative contracts; and discrimination by algorithms.

First, as information economics has shown, market mechanisms only function effectively if participants can make an—at least moderately—informed choice.[19] When it comes to the collection and processing of personal data by companies, many clients do have a vague notion of having lost control over their data,[20] and would strongly prefer that less data be processed by companies.[21] However, empirical studies show that almost nobody reads online privacy notices. A recent study demonstrated complete disregard of privacy notices, even in the case of an online application requesting highly sensitive information (risky sexual behavior), and even though the notices had been designed according to best practices to ensure maximum attention and ease of reading.[22] In theory, an informed minority might be sufficient to prevent grossly unfair terms and conditions by sanctioning companies using them.[23] However, for privacy notices, empirical studies show that this informed minority does not exist.[24] Therefore, the market for terms and conditions concerning privacy is not adequately policed, and fails to deliver results that adequately respect users' preferences for privacy.[25] Some users are aware of this: as another field study

[14] Cormen et al. concisely note in their standard text book on algorithms: "Before there were computers, there were algorithms. But now that there are computers, there are even more algorithms, and algorithms lie at the heart of computing." (Cormen / Leiserson / Rivest / Stein (2009), at xiii).

[15] Goldfarb / Greenstein / Tucker (2015).

[16] Brynjolfsson / McAffee (2014); but see for a historical perspective: Gordon (2016) (claiming that the digital revolution does not match the industrial revolution and its potential for economic growth).

[17] On predictive analytics, see Gandomi / Haider (2015), 143.

[18] A fourth, highly relevant, digitally mediated market failure is the question of restraint of competition generated by the behavior of online platforms; see, e.g. Evans / Schmalensee (2015).

[19] For an overview, see Stiglitz (2000).

[20] Pew Research Center (2014), 3: more than 90% of US adults think consumers have lost control over the online collection and use of data by companies.

[21] Madden / Rainie (2015), 9.

[22] Ben-Shahar / Chilton (2016).

[23] Schwartz / Wilde (1979), 637-638.

[24] Bakos / Marotta-Wurgler / Trossen (2014), 32.

[25] Even the *ex post* control of terms and conditions by the courts – as in the EU, instituted by the Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ 1993, L 95/29, – does not prevent widespread collection, analysis and sharing of personal data by companies such as Facebook or Google in the EU.

found, about half of the users have a fairly accurate understanding of Facebook's terms and conditions concerning privacy (despite not having read them)[26]; but even those rarely act on their knowledge. Despite the availability of cost-free encryption or IP hiding software, people are giving away personal data in unprecedented ways,[27] against their stated preferences. This leads to a gaping attitude-action gap concerning privacy protection.[28] The combination of the failure of sanctioning mechanisms for privacy-harming terms and conditions with the failure of users to act on their stated preferences gives rise to the often-deplored widespread processing of personal data by companies such as Google or Facebook.

One explanation for this attitude-action gap is the lack of alternatives, for example when network effects create a highly attractive dominant player such as Facebook.[29] However, behavioral science research suggests another potential source for users' passivity. In a recent empirical study, Alessandro Acquisti and colleagues inquired into the need for privacy in terms of the human instinct to avoid danger.[30] They argue that the need to protect one's privacy is triggered by visceral cues of the presence of strangers. Such presence makes us feel uncomfortable and wary of our privacy, but only if the presence is physical. The authors were able to show that the physical presence of a confederate, in the same or an adjacent room, made online disclosure of sensitive information by the participants less likely. Thus, offline sensorial cues can affect online privacy behavior. However, we are mostly alone when browsing the Internet, lacking sensorial cues that help us manage privacy in the offline world. Since people feel less threatened in solitary online environments, they exhibit less caution, and feel less of an urge to act on their stated privacy preferences, than in offline scenarios. The findings of Acquisti and colleagues therefore point to an important difference between the behavior of market participants in online and offline markets. If it is true that our evolutionary response mode to threats has adapted to the physical presence of threatening cues, such as strangers, the online environments of the digital economy will potentially catch users "off guard" more often than their brick-and-mortar counterparts. The widespread sharing of personal information vis-à-vis digitally operating companies, against the professed preferences of users, strikingly illustrates this property of online markets.

A second instance of digital market failure is derived from asymmetrical information: exploitative contracting.[31] In the world of Big Data, firms often know better

[26] Ayres / Schwartz (2014), 600: 54% of users correctly answered "yes" to the question of whether Facebook, in the US, may do the following according to its terms and conditions: "An advertiser tells Facebook that it wants to post an advertisement targeted at 24-year-old women who live in Detroit and like Michael Phelps. You fit all of these criteria. Facebook may share this information with the advertiser so that you will receive its advertisement".

[27] Cf. Madden / Rainie (2015), 8-9.

[28] Hacker / Petkova (2016), 5.

[29] Cf. Frank / Cook (1995); Dou / Niculescu / Wu (2013).

[30] Acquisti / Brandimarte / Hancoc (2015).

[31] Bar-Gill (2012), Chapters 3 and 4, particularly at 217-223; Grubb (2009, 2015); Heidhues / Kőszegi (2010); Heidhues / Kőszegi / Murooka (2012); Kőszegi (2014), 1104-10.

how clients will behave in the future than clients do themselves.[32] For example, the American Banker tells us that

> [n]o other industry in the world knows consumers and their transaction behavior better than the bank card industry. It has turned the analysis of consumers into a science rivaling the studies of DNA. The mathematics of virtually everything consumers do is stored, updated, categorized, churned, scored, tested, valued, and compared from every possible angle in hundreds of the most powerful computers.[33]

And the manager of a leading mobile phone company in the US adds that "[p]eople absolutely think they know how much they will use [their cell phones] and it's pretty surprising how wrong they are."[34] As Kamenica, Mullainathan, and Thaler have argued, the superior knowledge of firms regarding the future behavior of their clients may lead to "adverse targeting", whereby offers are tailored to individuals in an attempt to exploit their specific weaknesses that become apparent in the data.[35] Ryan Calo notes that firms have an incentive to engage in individualized 'market manipulation' in which consumers are targeted based on their specific sets of biases or approached when they are at their most vulnerable.[36] Empirical studies tend to confirm these hypotheses, and show that such practices lead to significant welfare losses.[37] Such exploitative contracting therefore combines behavioral market failure with an asymmetry of computing power (access to Big Data analytics) to form a second sub-category of digital market failure.

Its third instantiation arises from the generation or perpetuation of discrimination by algorithms.[38] Again, standards of both efficiency and fairness are breached when algorithmic decision making systematically disfavors certain protected groups.[39] An emerging literature in computer science points to the difficulties of rooting out discrimination by algorithms.[40] Bias can enter the algorithmic processing of data in a number of ways. To bias selection processes, the coder may of course simply define and screen for discriminating target variables, for example those that are openly racially tainted. However, discrimination may arise in subtler, and often unintentional, ways, too. For example, the data set that an algorithm has to be trained on may be incomplete or skewed. Hence, the correlations found between certain independent variables and the target variable (the trait one is really looking for) are biased.[41] If, for instance, an algorithm is employed to screen candidates' suitability

[32] Kamenica / Mullainathan / Thaler (2011), 417.

[33] MacDonald (2007).

[34] Bar-Gill (2012), 35.

[35] Kamenica / Mullainathan / Thaler (2011), 418.

[36] Calo (2014), 1033.

[37] Op. cit. note 31.

[38] Barocas / Selbst (2016); Hacker / Petkova (2016); on discrimination as a market failure see Sunstein (1991).

[39] On discrimination and fairness, see, e.g., Caracciolo di Torella / Masselot (2004); on the more complex case of efficiency, see, e.g., McCaffery (1993), 648-651; Donohue (1989).

[40] See, e.g., Calders / Žliobaitė (2013); Calders / Verwer (2010).

[41] See, e.g., Barocas / Selbst (2016), 680-687.

for jobs, it will likely be trained on a data set containing previously successful candidates. However, if for historical reasons most of these successful candidates were white males, the screening of new candidates will result in a disproportionately high number of white males being classified as good candidates.[42] Furthermore, the target variable may not only positively correlate with the desired trait of a person (suitability for a job; fitness; eligibility for a contract), but also negatively with membership in a certain protected group.[43] This allows for bias to be intentionally (if the coder knows of and uses these dual correlations) or unintentionally (if the coder does not previously know of these dual correlations) introduced into the algorithm. Evidence is mounting that such concerns are not purely theoretical, but do affect real-world decisions to the detriment of certain, marginalized groups.[44] Such discrimination is made possible, in part, by users' willingness to share sensitive, personal information online, as noted before.

The three instances of digital market failure just reviewed all specifically connect to data-driven or online markets. In some cases, they are mediated by the special characteristics of online environments to which users react differently than to offline environments (privacy "attitude action gap"; discrimination by algorithms). In other cases, they (also) replicate some of the market failures known from offline markets, but are potentially exacerbated by the qualitatively new imbalances of power created by vastly differing access to computing power and algorithms (exploitative contracting) and the current lack of effective public scrutiny and regulation (discrimination by algorithms).[45] As more and more decisions are left to algorithms, we must ensure that the law affords adequate protection against their negative main or side effects, while not, at the same time, unduly stifling innovative technologies and market applications.

3 The Promise of Personalized Law

What is also becoming apparent in these data sets, and in related empirical studies, is that people differ vastly in their preferences, capacities, and behavior.[46] This heterogeneity entails different degrees of vulnerability vis-à-vis digital market failure. Some people simply do not care about privacy, others do know about potential perils and protect themselves; some people are not easily fooled by individualized offers and are able to navigate, and even benefit from, potentially exploitative contracts; and some people are less likely to be discriminated against. This type of actor heterogeneity poses a serious problem for current approaches to regulation, both in

[42] For an early example of this see Lowry / Macpherson (1988).

[43] Hacker / Petkova (2016), 7-9.

[44] See, e.g., Sweeney (2013); Barocas / Selbst (2016); cf. also Rosenblat / Levy / Barocas / Hwang (2016).

[45] Cf. op. cit. note 38; cf. also Edelman / Luca / Svirsky (2016), 4, 23-24.

[46] Stanovich / West (2000); Schwartz (2015), 1393-1395; Hacker (2017), Part 1.

offline and online markets. If people differ in their behavior and capacities, a one-size-fits-all solution (e.g., mandating the same disclosures for all consumers) will be overprotective for some and underprotective for others.[47] Therefore, some scholars are suggesting personalized laws.[48] The general idea is to use available data about citizens in order to tailor laws to their specific needs and capacities. In the context of the regulation of data-driven markets, the hope would be to address digital market failure precisely where it is most likely to arise.

Such personalization may take different forms, but will mostly consist of five consecutive steps. First, subjects have to be categorized along a desired, meaningful metric. For example, Ariel Porat and Lior Strahilevitz have suggested using information on psychological personality traits (specifically, the dimensions psychologists call the Big Five: openness, conscientiousness, extraversion, agreeableness, and neuroticism) to sort people into different categories.[49] The Big Five are abstract, scaled constructs which, in spite of all the criticism they have drawn,[50] offer the current leading theory of classifying personality types in personality psychology.[51] Using Big Data, such information can be obtained from seemingly innocuous data patterns. For example, Chittaranjan, Blom, and Gatica-Perez were able to establish correlations between these personality traits and specific patterns of smartphone usage[52]—data that every cell phone company already collects.[53] It was possible to make strong inferences from the number of incoming and outgoing calls, their length, the frequency of the use of the YouTube app, and of communication via email and text message, as well as other types of metadata. For instance, the study showed that extraversion correlates with a higher number of incoming calls and their longer duration. In fact, such inferences from metadata have proven to be more accurate predictors of personality traits than classical psychological personality trait tests.[54] Similar studies exist for behavior on social networks such as Facebook.[55] However, different metrics, such as the degree of bounded willpower, the degree of certain biases, wealth and income, or credit scores, may also be used for the purpose of personalization.[56]

Second, a "general personalization law" must establish, in the abstract, the legal consequences of the different scores for those situations in which law is to be

[47] Cf. Hacker (2016b).

[48] Porat / Strahilevitz (2014); Ben-Shahar / Porat (2016); Sunstein (2013); Busch (2016); see also Hacker (2016b).

[49] Porat / Strahilevitz (2014).

[50] Block (1995).

[51] See McCrae / John (1992), 181; Gosling / Rentfrow / Swann Jr. (2003), 506; John / Srivastava (1999), 103.

[52] Chittaranjan / Blom / Gatica-Perez (2013).

[53] Bar-Gill (2012), 33 and Chapter 5.

[54] Staiano / Lepri / Aharony / Pianesi / Sebe / Pentland (2012).

[55] Back / Stopfer / Vazire / Gaddis / Schmukle / Egloff / Gosling (2010); Porat / Strahilevitz (2014), 1439.

[56] Hacker (2016c).

personalized. For example, it could require, in disclosure obligations, tailored salience of potentially exploitative contractual features, depending on how relevant this information is likely to be for the recipient. Before the formation of a credit card contract, people scoring high on a number of relevant biases (the "uncalibrated" type) would receive prominent warnings about, for example, high interest rates kicking in after teaser rates expire, while more rational actors (the "well-calibrated" type) would not receive such warnings. Or, to pick another example, think of cell phone tariffs: an uncalibrated actor could be informed in a salient way about high back-end fees, which are due once the monthly budget of minutes is used up. By contrast, the well-calibrated actor, who practically always remains within the bounds of her estimated future phone communication behavior, would be informed in a salient manner about the costs of the regular tariff excluding overconsumption fees.

Third, some entity must subsume the concrete, individual scores under the requirements of the general personalization law. This procedure would determine that for actor A, with score x, legal consequence L_x is triggered; for actor B, with score y, legal consequence L_y; for actor C, with score z, legal consequence L_z etc. This concrete application of the general personalization law (which only defines the legal consequences for all different actor types in general) can be conducted by a company or a government regulatory agency. Company-based personalization might make sense if companies already lawfully collect the relevant data in any case. The downside is that it is difficult to monitor whether companies correctly execute the law. Government-based personalization, by contrast, requires some agency to get access to the data (either by conducting empirical studies or by requiring companies to disclose data). This, in turn, invites concerns of privacy protection and potential abuse of the data. I take up these challenges in detail in the next section.

Fourth, the relevant scores must be stored and updated as new data becomes available. In a companion paper,[57] I suggest that, at least for government-based personalization, the blockchain technology can be used to create a decentralized, pseudonymous "legal blockchain" containing all relevant parameters for government-based personalization. Finally, fifth, the scores must be communicated to citizens in ways that enable them to know what "their" personalized law is. A smart phone app or a website could display the relevant personalized law to the individual citizen. Moreover, this personalized version of the law of a specific citizen must also be communicated to prospective counterparties, for example before contract formation, so that disclosures can be adapted, and individualized default or mandatory rules taken into account.

All in all, personalized law promises to use digital technology, and particularly Big Data analytics, in an attempt to mitigate online and offline market failures while at the same time maximizing freedom of contract for those not in need of specific forms of regulatory protection. In the context of this chapter, it therefore presents a possible way forward to square the maintenance of an environment for innovation

[57] Hacker (2016c).

in the digital economy with the need for protection of some, but not all, participants in data-driven markets.

4 The Legitimacy of Personalized Law

The preceding section has shown how personalized law can be operationalized in theory. If implemented, it would amount to a massive reconfiguration of the design of lawmaking. A number of proposals for personalized law, ranging from disclosures and nudges, such as default rules and debiasing, to mandatory law, have been put forward in the literature.[58] However, what is lacking is a comprehensive assessment of the legitimacy of personalization. This is what the remainder of the chapter undertakes.

Perhaps the best-known contemporary theory of legitimacy in law was elaborated by Jürgen Habermas, who argued that valid, i.e., legitimate, norms must be supported by reasons that all of the affected persons can assent to.[59] If personalized law is implemented as an opt-in or opt-out tool that citizens are free to use or not to use, this very assent (or non-objection in the case of opt-out) is written into the code of personalizing strategies. Nevertheless, and independently of the registered opinion of data subjects on personalizing their law, such a regime must be supported by normatively defensible arguments. It is insufficient, particularly in view of cognitive default effects,[60] to point to the mere possibility of citizens' choice as a strategy for legitimation. Therefore, understanding legitimacy in a contextualized sense, I ask whether personalization can be squared with key doctrines of positive law, equality and justice, and legal and democratic theory as they stand. Only if these questions can be answered in the affirmative can personalized law truly claim to be a legitimate instrument of lawmaking. In this endeavor, the following sub-sections first deal with challenges stemming from positive law, then with matters of equality and justice, and finally with legal and democratic theory.

4.1 Challenges Posed by Positive Law

As regards positive law, personalization first and foremost raises serious concerns of data protection. Conversely, those in possession of the data must be trusted to adhere to restrictions laid down in positive law, and in particular not to use the data for illegitimate purposes. This is of particular concern when the government is processing data.

---

[58] Op. cit. note 48.

[59] Habermas (1996), 110.

[60] Samuelson / Zeckhauser (1988).

4.1.1 Data Collection and Data Protection

Personalization necessitates the availability of personalized data. Personalizing law would further cement the collection of data instead of reining in these practices for reasons of privacy, as provided for by Art. 8 of the European Charter of Fundamental Rights. At the most general level, however, it is submitted that the attempt to use Big Data for the benefit of the data subject follows the exhortation of Recital 4 of the General Data Protection Regulation (GDPR) that data collection should serve mankind. However, we have to distinguish between government-based and company-based personalized law. The latter would attach legal consequences only to data which is already being lawfully processed by companies, in an attempt to prevent them from unilaterally benefiting from data mining. Therefore, it raises no *additional* concerns about data protection independent of those created by the current practice of data collection.[61] Government-based personalization, by contrast, does generate novel concerns about privacy. Data has to be collected, directly or indirectly, by a government agency, processed, and linked to the legal consequences personalized law specifies. All of these actions therefore need to be provided for in a general piece of legislation, as stipulated by Art. 6(3) GDPR. If an opt-in or opt-out regime is chosen, the right to object to profiling, Art. 22(1) GDPR, is respected. If, however, personalization is mandatory, Art. 22(2)(b) GDPR requires that "suitable measures [be taken] to safeguard the data subject's rights and freedoms and legitimate interests". This brings us to the second key issue, the question of data security and the possibility of abuse.

4.1.2 Data Use and Data Abuse

The disclosures by WikiLeaks, hacker attacks on Sony,[62] Yahoo,[63] and Uber[64] and the proliferation of credit card data being published in the dark web show[65] that full data security cannot be guaranteed even with the most advanced techniques of encryption. The more data are distributed, the more they can be decoded and put to malevolent use. The external threat by hackers is paralleled by an internal one. Even those legitimately in possession of data—be it companies or a government agency—may abuse it. In company-based personalization, companies who would legitimately harvest data will often have a pronounced interest in exploiting these sources of knowledge to their own benefit. Moreover, associated with government-based personalization is the dystopia of an all-controlling, psychologically manipulative state. Again, it is the latter variety of personalization which raises most novel concerns with respect to the abuse of data, as the potential for abuse in a

[61] For an account of these concerns, see, e.g., the contribution by Oostveen / Irion in this volume.

[62] Franceschi-Bicchierai (2016).

[63] Perlroth (2016).

[64] PYMNTS (2016).

[65] Schwindt (2016).

company-based framework of personalization is not greater than under current conditions—companies would not be allowed to collect more data, but rather be required to use the data they collect differently. However, if *governments* via personalized law have *increased* access to profiling data about their citizens, they must be trusted to adhere to Art. 5(1)(b) GDPR, which holds that personal data shall be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes". In other words, if data is collected for the purpose of, for example, personalizing usury laws, the used scores may never be harnessed for other legal actions, such as procedures of criminal prosecution, or for tailored political campaigning.

Pseudonymization can help in this endeavor,[66] since hackers or insiders obtaining pseudonymous information cannot link the data to specific data subjects unless they are also in possession of the separate information allocating pseudonyms to real names. However, since such a list must exist, it is not inconceivable that it could be stolen by external intruders, or abused by government insiders; de-pseudonymization is not impossible. The strict adherence to the letter of the data protection principles of the GDPR, such as Art. 5(1)(b), therefore presupposes the functioning of the *Rechtsstaat*, and the monitoring of potential abuses by independent civil organizations and the media. The key problem with these presumptions is that we cannot guarantee that they will be fulfilled at every moment of the existence of personal information in the hands of the government. Even though many Western countries at the moment might, with the right safeguards, checks and balances in place, be trusted to use personalization data only for their lawful purposes, political majorities may change over time. In fact, the rise of authoritarian forms of government in several European countries over the last few years, including the attempt to dismantle the *Rechtsstaat* and to disable the monitoring functions of civil society,[67] shows that this is not a purely theoretical concern. The potential use of personality trait information for political agendas, and arguably propaganda, is further evidenced by the extensive use of personalized voter mobilization and voter suppression techniques, tailored via personality trait information, by the Brexit and Trump campaigns, which may have had a significant impact in both political contests.[68] Hence, government-based personalized law must be designed so that even in the hands of an authoritarian government, negative consequences for citizens are limited. This implies that highly sensitive information, which is rich in, or can be correlated with, highly predictive and encompassing psychological traits, should be

[66] "'[P]seudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person", Art. 4(5) GDPR.

[67] See, e.g., Fomina / Kucharczyk (2016); Ágh (2015); see also the interview with the Presidents of the German and French Constitutional Courts, Janisch, W. / Ulrich, S. (2016), "Die EU muss klar Position beziehen", Süddeutsche Zeitung of 21 October 2016 (hyperlink only in Reference List).

[68] See, e.g., Grasegger / Krogerus (2016); for a skeptical view of the effectiveness of psychometric political targeting, see Karpf (2017).

avoided in government-based personalized law. *In concreto*, information about personality traits should not be explicitly used or stored.

In sum, the potential for abuse necessitates a trade-off between predictive accuracy and data security. Data sets which enable highly accurate predictive analytics over a wide variety of actions are attractive for personalized law as they allow for precise tailoring along a range of metrics. However, simultaneously, they generate the most concerns with respect to abuse. These tensions between accuracy and potential abuse will have to be resolved in every concrete instance of personalization. However, personality trait information is so comprehensive and linked with so many other features of behavior[69] that we should, as a general preventive measure, not use it for government-based personalization.

4.2 Equality and Justice

The legitimacy of personalized law not only concerns possible frictions with data protection law, but also conjures up questions of equality and justice. In essence, personalized law is about treating different people differently. Paradoxically, I argue, consciously designed personalization may further equality before the law and distributive justice.

4.2.1 Two Dimensions of Equality Before the Law

Legal equality, which after all is a normative pillar of modern Western law,[70] at first glance might seem to be at odds with personalization. If this were true, personalization would be difficult to justify. Moral and political philosophy hold equality in high regard,[71] and for centuries, citizens have fought for everyone to be treated equally before the law.[72] As Michael Stolleis remarks, the invocation of legal equality has increased

[69] See, e.g., Carney / Jost / Gosling / Potter (2008) (relating personality traits to political orientation); Barrick / Mount, (1991) (relating personality traits to job performance); Wiggins / Pincus (1989) (linking personality traits to personality disorders); for an overview see John / Srivastava (1999), 121, 125; see also the preceding footnote.

[70] See only Meenan (2007), 17; Kirchhof (2015), para. 1: "Elementarregel" [most basic rule]; Stolleis (2003), 8-10; see also Smith (2011), Chapter 1.

[71] See already Aristotle, *Politics*, Book III, § 12, 1282b14: "it is therefore thought by all men that justice is some sort of equality"; also in the *Nicomachean Ethics*, Book V, § 3, 1131a10; Pojman / Westmoreland (1997), 1; Kymlicka (2002), 3-4; Sen (2009), 291-292; as Amartya Sen, following Aristotle (id.), has rightly noted, however, the question is always: "Equality of What?", Sen (1980); see also Rawls (1999a), 447, noting the distinction between "equality as it is invoked in connection with the distribution of certain goods, some of which will almost certainly give higher status or prestige to those who are more favored, and equality as it applies to the respect which is owed to persons irrespective of their social position".

[72] For an illuminating historical perspective, see Stolleis (2003); Pöschl (2008), Part B; and, regarding equality as a principle of private law, Grünberger (2013), Part 1.

dramatically from the Enlightenment on, particularly since the French Revolution, when the erosion began of the old estate-based system, which rested on categorical, theologically and politically entrenched inequality between social classes.[73] Personalization seems to reverse this emancipatory move by treating people radically differently again. Can personalization hence be squared with legal equality? I claim that it can and that, even more, equality sometimes even demands personalization.

4.2.1.1 Equality of Sanctions

Following Aristotle's canonical distinction between distributive and corrective justice,[74] two concepts of equality can be distinguished that are relevant for private law. One strives for formal equality, the same legal consequences for everyone; the other aims to justify necessary distinctions between persons. Both can be traced back to classical treatments by Aristotle; we can uncover the first root of legal equality in Book V of the Nicomachean Ethics, in a passage in which the Stagirite discusses corrective justice:

> For it makes no difference whether a good man has defrauded a bad man or a bad one a good one, nor whether it is a good or a bad man that has committed adultery; the law looks only at the nature of the damage, treating the parties as equal, and merely asking whether one has done and the other suffered injustice, whether one inflicted and the other has sustained damage.[75]

This idea of disregard of the person inspired legal theorists to call for the abolition of legal privilege,[76] and for the uniform application of laws to all subjects.[77] The same law should govern irrespective of the personality and, more importantly, moral worthiness, wealth or social status of the persons in question.

Personalization may be considered to stand in stark contrast to this variety of equality. However, it is not without reason that Aristotle restricts his observation to sanctions (and measures of exchange). Throughout history, and particularly in contemporary law, different laws have governed people in their different roles in society. After the revolutions of the eighteenth and nineteenth century, strict, formal equality before the law perhaps saw its heyday in late-nineteenth century laissez faire contract law, which granted formally the same freedom of contract for all but led to highly different economic outcomes, as is well known.[78] But today, it has

---

[73] Stolleis (2003), 8-10, 15.

[74] Aristotle, *Nicomachean Ethics*, Book V.

[75] Aristotle, *Nicomachean Ethics*, Book V, § 4, 1132a2.

[76] Kirchhof (2015), para. 4.

[77] Stolleis (2003), 14-15; Cancik (1998).

[78] While the law formally guaranteed legal equality and freedom of contract for all, the tools of the law have served different groups in different ways. As legal historian Franz Wieacker notes, the formality of the concept of freedom of contract, and its abstraction from real differences in economic endowments, cognitive capacity, or social vulnerability, opened opportunities for the trade-savvy, commercial upper and middle class while tending to leave those unfit for the smart game of

receded to the treatment of compensation, where a majority of scholars sees just compensation as restoring the previously existing or contractually agreed balance of goods, independent of any individual characteristics of the parties involved.[79] If a poor man breaks a jar, he has to pay as much as a rich man.[80]

4.2.1.2 Equality as Reasoned Difference

In most other domains, however, strict legal equality, in the sense of "one law for everyone", as championed by the French Revolution,[81] has long been abandoned, or rather, never existed in the first place. Specific rules govern different subgroups of citizens, particularly in private law. Consumers are subject to special mandatory provisions; disclosures are different for retail and professional investors[82]; *diligentia quam in suis* holds actors accountable for different levels of care[83]; and in German law, only some entrepreneurs, typically those with larger undertakings (*Kaufmänner*), are subject to the Commercial Code.[84] In most cases, these special provisions are justified by an assumption of different degrees of sophistication, vulnerability, or experience between different market participants. Again, Aristotle, this time discussing distributive justice, provides an early formulation of the idea of special treatment when there are reasons for distinguishing some citizens from others.[85] His famous example is that when it comes to playing the flute, those best at flute-playing should be given the best flutes, irrespective of their birth, beauty, or wealth.[86] Such an understanding of equality—giving "like to likes", and "unlike to unlikes"—has been criticized in contemporary political philosophy[87]; nevertheless, it is reflected in

---

the market behind (Wieacker (1967), 441 et seq., and 462; see also id., 543 et seqq.). Thus, the steady adherence to the concept of legal equality, particularly in its variety of formal equality to contract, correlated with the increasing inequality of economic outcomes.

[79] Oetker (2016), para. 8; Jansen (2005), 162-163 (explaining the compensation principle of civil liability as a direct consequence of late scholastic adaptations of Aristotle's theory of corrective justice).

[80] Only extreme cases limit this principle such as outright psychological disorders exempting a person from responsibility.

[81] See Stolleis (2003), 16.

[82] Cf. Art. 30(2) of the Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments (MiFID II), OJ 2014, L 173/349, which governs "counterparties", a subgroup of professional investors.

[83] See, e.g., §§ 708, 1359, 1664(1) of the German Civil Code (BGB).

[84] § 1 Handelsgesetzbuch (HGB).

[85] Aristotle, *Nicomachean Ethics*, Book V, § 3, 1131a10; *Politics*, Book III, § 12, 1282b14.

[86] Aristotle, *Politics*, Book III, § 12, 1282b14.

[87] Westen (1982), 547-548 (critique of tautology); Smith (2011), 24 (critique of incompatibility with modern egalitarianism). Particularly, of course, Aristotle and the society he lived in did not subscribe to the modern view of equal liberty and rights for, or worthy of, all persons (Deslauriers, 2013). Distributive justice governing the distribution of goods and obligations, for Aristotle, requires proportionality, and proportionality in turn is measured in terms of *axia* (ἀξία), or (differing) moral worthiness (Aristotle, *Nicomachean Ethics*, Book V, § 3, 1131b10-15).

the current understanding of legal equality governing the distribution of legal obligations, as formulated by the Court of Justice of the European Union: "as the Court has consistently held, discrimination consists solely in the application of different rules to comparable situations or in the application of the same rule to differing situations."[88] Importantly, thus, legal equality of this second variety not only demands the treatment of comparable situations in the same way, but also the treatment of different situations differently. This view is shared by most of the contemporary legal literature,[89] the European Court of Human Rights,[90] and by the German[91] and Austrian Constitutional Courts,[92] for example. This second formulation of equality seems defensible precisely because it asks us to inquire into, to discuss, and to evaluate the reasons for treating people differently—which is partly what legal order is about.[93] In order to uphold legal equality, it is thus necessary to determine whether two situations are comparable or different, which in turn necessitates arguments in favor of or against the differentiation. However, legal scholarship has so far mostly focused on the first part of this variety of equality, the differential treatment of comparable situations. Personalization brings the second part into focus. Under such a lens, personalized law must be judged on whether the metrics it uses to differentiate between actors can legitimize differential treatment.

4.2.1.3 Personalization and Equality

As explained, the metrics of personalization would measure the real behavior, and thus approximate the real needs, of citizens, and tailor laws accordingly. Insofar as these metrics—such as the degree of rationality, vulnerability, or economic background—are relevant to the purpose of the norm, it seems that legal equality in the second sense would even require personalization. While current law only operates with *assumptions* about these important parameters, and thus cannot adequately cope with actor heterogeneity, personalized law promises to inject *empirical rigor* into the design of lawmaking. If this helps to more effectively deploy the purpose of the law by matching its effects with those for whom the effect is most beneficial, the

---

[88] ECJ, Racke v. Hauptzollamt Mainz, C-283/83, ECLI:EU:C:1984:344, para. 7; repeated in ECJ, Finanzamt Köln-Altstadt v. Schumacker, C-279/93, ECLI:EU:C:1995:31, para. 30; see also ECJ, Kingdom of Spain v. Council of the European Communities, C-203/86, ECLI:EU:C:1988:420, para. 25.

[89] Meenan (2007), 21; Allen (2007), 46; Kirchhof (2015), para. 3, 7 and 8; Pöschl (2008), 159; Tridimas (2006), 62; for a critique, see Westen (1982).

[90] Allen (2007), 46.

[91] BVerfGE 55, 72 (88) – Präklusion (Vereinfachungsnovelle); BVerfGE 92, 365 (407) – Kurzarbeitergeld.

[92] Pöschl (2008), 158-159.

[93] Kirchhof (2015), para. 5; Pöschl (2008), 140-141; cf. also Smith (2011), 114 and 24: "equal treatment and different treatment both require justification"; Waldron (1991), 1358-1361 (offering a good example of such justificatory argumentation).

differentiation uncovers legally relevant differences so that equality before the law, in its second meaning, is ultimately strengthened.

Thus, it is really equality in the first sense mentioned, as an equality of sanctions and remedies independent of the individual traits of the parties, which would be challenged by a personalized regime (of compensation). As Bilyana Petkova and I have argued,[94] however, taking personal traits into account may help to equalize the effect of laws by adapting deterrence to individual tolerance of sanctions. This is most obvious with income and wealth, whose differential distribution clearly distorts the deterrent effect of monetary fines and damages; in many European countries, for example, but not in the US,[95] this is partially recognized by adapting criminal fines to the level of income (but not wealth) of defendants through so-called day fines.[96] By extension, even in the domain of sanctions the principle of just compensation derived from Aristotelian corrective justice ought to be balanced with a modern understanding of sanctions serving not only corrective justice *ex post* but also deterrence *ex ante*.[97] Personalization is a promising way forward along this path, stressing equality of the *effect* over equality of the absolute *amount* of compensation and sanctions.

4.2.1.4 Stigmatization

Nonetheless, just as a one-size-fits-all approach, while maintaining formal equality, has invited material inequality,[98] personalization, while safeguarding material equality, may invite a perceived sense of formal inequality. Citizens may resent being classified and subjected to special treatment, even if they might benefit from such personalization along a range of parameters. Ultimately, for example, citizens subject to special forms of protection because of their low cognitive capabilities or low economic endowments might feel stigmatized, even if personalized law is passed with the best intention to help them.[99] Thus, they might feel treated unfairly and unequally. There are four answers to this problem. First, it must be pointed out that the category a citizen is sorted into is not fixed, but rather fluid. As soon as the relevant parameters change, the classification will change alongside them. Therefore, as a matter of theory, no one would be "locked in" to a certain category. Second, wherever possible, laws should be designed so as to facilitate in practice the move from one category to the other, for example by providing learning opportunities (e.g., for changing degrees of rationality)[100] or by opening ways out of poverty.

---

[94] Hacker / Petkova (2016).

[95] Kantorowicz-Reznichenko (2015), 485.

[96] See, e.g., § 40 Abs. 2 of the German Penal Code (StGB), which links the amount of a criminal fine to the daily income of the perpetrator.

[97] Cf. Posner (2014), 223.

[98] Op. cit. note 78.

[99] Porat / Strahilevitz (2014), 1433, 1462-1464.

[100] Hacker / Dimitropoulos (2017).

Third, potentially stigmatizing categories, such as degrees of rationality, or personality types, should be used with care and only employed if they can be expected to make those who might feel stigmatized substantially better off, providing them with reasons to assent to this type of personalization.[101] Finally, if concerns about stigmatization are particularly virulent, an opt-in or opt-out regime should be employed to ensure that those who feel highly uncomfortable with being allocated to one of the proposed categories can withdraw from the personalization regime. Personalization should only be mandatory if legitimized by significant negative externalities, such as in the case of personalized negligence law.[102] By contrast, when the main purpose of the law is paternalistic, rather than the prevention of negative externalities, a voluntary regime of personalization (opt-in or opt-out) seems preferable.

All in all, legal equality does not prevent us from legally differentiating between persons, but it does require us to justify this with good reasons. Personalization along relevant parameters therefore may further legal equality, particularly understood in material terms, i.e., with reference to the real effects of laws for citizens. However, to mitigate a possible sense of stigmatization, opting in or out of personalization regimes should in principle be possible unless this generates significant negative externalities.

4.2.2 Distributive Justice

The questions of legal equality and distributive justice are interconnected, as we have already seen in the brief discussion of Aristotle. Nevertheless, an important difference of focus remains at the outset. While legal equality asks us to consider the reasons brought forward to justify differential (or equal) treatment in each and every case, distributive justice explicitly addresses the overall allocation of socio-economic goods in society.[103] With levels of economic inequality rising,[104] policies are coming under increasing pressure to be justifiable in terms of distributive justice as well. In fact, with populism *en vogue* both on the left and the right end of the political spectrum,[105] distributive justice may prove to be one of the most important political, and legal, categories of the decades to come. Therefore, distributional concerns should not be absent from an assessment of legitimacy of personalized law.

Theories of distributive justice abound.[106] Depending on the normative yardstick chosen, personalized law is judged in different ways. Ben-Shahar and Porat, for

[101] See op. cit. note 59 and accompanying text.

[102] Ben-Shahar / Porat (2016).

[103] Cf. Rawls (1999b), 130.

[104] Piketty (2014); Bourguignon (2015); despite all controversies revolving around Piketty's thesis on the *cause* of rising inequality ($r > g$), the fact of rising income and wealth inequality itself seems to be well established; see, e.g., Jaumotte / Lall / Papageorgiou (2013), 276-277 (on income inequality); Saez / Zucman (2016) (on wealth inequality).

[105] Judis (2016).

[106] Fleischacker (2004).

example, examine their concept of personalized negligence law from a distributive perspective geared towards socio-economic equality.[107] By contrast, I would like to briefly discuss the implications of one particularly noteworthy, perhaps the most important contemporary theory of distributive justice[108]: that formulated by John Rawls. Famously, he asks how free and equal citizens in what he terms the "original position", i.e., behind a veil of ignorance concerning their future position in society, would set up the basic structure of a just society.[109] He claims that they would coincide in the elaboration of a list of principles of justice.[110] In his own words:

(a) Each person has the same indefeasible claim to a fully adequate scheme of equal basic liberties, which scheme is compatible with the same scheme of liberties for all; and
(b) Social and economic inequalities are to satisfy two conditions: first, they are to be attached to offices and positions open to all under conditions of fair equality of opportunity; and second, they are to be to the greatest benefit of the least-advantaged members of society (the difference principle).[111]

The important distributive criterion is found in the difference principle. In every piece of lawmaking, it asks us to maximize the benefits for those worst off. Rawls offers a number of strong arguments for this principle. First, he claims that other principles (such as expected utility maximization/utilitarianism) cannot prevent catastrophic outcomes, as they may always be offset by the greater gains of some other group; the difference principle, by contrast, ensures a maximal "security level".[112] Second, the difference principle is informationally parsimonious, as only an ordinal ranking of (worst) outcomes is required, and not a cardinal ranking.[113] Third, by not aggregating costs and benefits over different citizens, it takes differences between persons seriously.[114] This highly normative claim is anchored in a Kantian understanding of the person and, following from this, the refusal to treat an individual as a mere end (for welfare maximization).[115] Fourth, and perhaps most importantly, the difference principle minimizes social inequality and fosters social coherence by offering arguments to already marginalized groups.[116] This seems to be of particular importance in an age in which inequality is rising,[117] and the political

[107] Ben-Sahar / Ariel Porat (2016), 39-41; they remain silent, however, about the exact theory of distributive justice they employ but their examples show that they would be reluctant to exacerbate existing levels of socio-economic inequality.

[108] Cf. Miller (2003), 87 and 89.

[109] Rawls (1999a), Chapter 3.

[110] Rawls (1999a), Chapter 2.

[111] Rawls (2001), 42-43; cf. also Fleischacker (2004), 110.

[112] Rawls (1999a), 134.

[113] Rawls (1999a), 79.

[114] Rawls (1999a), 87-88.

[115] Kant (1785), AA IV, 428.

[116] Rawls (1999a), 88; see also Rawls (1974), 144-145.

[117] Op. cit. note 104.

repercussions of (perceived) marginalization and exclusion are being felt ever more clearly, be it in the Brexit vote[118] or in the rise of right-wing populism.[119] Strategies adhering to the difference principle can always claim that, given the policy options, they did maximize the position of the worst off; such arguments can be expected to be more acceptable to the least-advantaged members of society than other discourses of legitimization.

Adhering to the difference principle in each and every political decision is virtually impossible. However, personalized law offers a perspective to reinstate some of its contents in market regulation. Specifically, particular forms of protection and/or of opportunities can be tailored to those with the worst credit scores or the lowest degrees of rationality. For example, overdraft regulation in the US, currently a hot issue in the EU as well,[120] was shown to be largely ineffective for those most in need of it, namely poor account holders potentially entering into debt spirals through overdraft charges.[121] Strengthening protection for these groups, by making overdraft charges contingent on qualified forms of consent, or by capping charges, may make a meaningful contribution to market regulation while simultaneously furthering distributive justice under the difference principle.

As with every regulatory tool, personalization can be harnessed for different normative goals. Its unique potential to single out specific actors in need of special protection, however, makes this tool particularly appealing for theories of distributive justice that favor the improvement of the lot of those worst off in society.

4.3 Challenges Posed by Legal and Democratic Theory

Beyond the burdens of equality and justice, personalized law also gives rise to major questions relating to legal theory and democratic discourse. On the one hand, the expressive function of the law might be threatened by the dominance of an atomistic concept of the law that does not seem to express universal values anymore. On the other hand, an elaboration of laws conceived in technological, complex, and even algorithmic terms will pose new challenges to democratic discourse.

4.3.1 Loss of the Expressive Function

Personalization changes the deep structure of the law. It fragments the block of legal norms, which was a hallmark of the idea of codification in the nineteenth century and before, and which has until now remained rather monolithic.[122] Rules that were

[118] Becker / Fetzer / Novy (2016).

[119] See Judis (2016).

[120] CMA (2016).

[121] Willis (2013).

[122] See, e.g., Wieacker (1967), 475 et seqq., 459 et seq., particularly 462.

supposed to have universal value are, when subjected to personalization, converted into a decentralized network of norms created by humans but fed and ultimately refined by algorithms. The norms are attached to different metrics, which in turn depend on data networks. It might seem as if the only connecting element between the different parts of the network, the different data-reactive norm structures, is the algorithm that conducts the necessary allocations and updates them in a purportedly disinterested manner. Such de-collectivization of the normative apparatus might lead to the loss of something that has been described as the expressive function of the law[123]: the idea that uniform, publicly accessible legal norms go beyond the provision of the maximally precise or efficient solution of specific problems by expressing simultaneously a legally binding minimal ethical theory, a consensus, however imperfect, about good action. In spite of all the complex interactions between ethical theory and the law, which cannot be traced in this chapter, this postulate of a universal, ethical component of the law has an impressive pedigree that, again, harks back to Aristotle.[124] Thus, for example, antidiscrimination law can be seen not only as a regulation of business conduct but also as an expressive sign that discrimination is generally not tolerated in our society. Does this expressive function stand to be lost as laws are increasingly particularized, personalized, de-universalized?

It is true that, if personalization is applied, the one "single law" which applies to all circumstances will no longer exist. However, as noted above, such laws are even now rather the exception than the rule. Already, laws are being created for ever more refined subgroups (e.g., consumers; founders of new businesses[125]; minors[126]; those unable to take care of their own affairs[127]; retail investors, professional investors, and counterparties under MiFID II[128]). These rules, far from expressing universal values, only define standards for certain communities within society. The monolithic approach to the law, promising one law of the land for everyone, is therefore already in full decline.

Nonetheless, personalized law does not reduce the declining expressive function of the law to zero. Rather, even with personalization, ethically grounded principles can be distilled from the most general allocations of legal consequences to certain metrics. For example, when special protection is afforded to bank account holders with low credit scores or highly bounded willpower, this decision is an expression of the refusal to let companies unduly profit from particularly vulnerable clients; the

[123] See, e.g., Sunstein (1996); Adler (2000); Anderson / Pildes (2000); Feldman / Orbel (2015).

[124] Aristotle, *Nicomachean Ethics*, Book V, § 1, 1129b14-25; today, prominent theories include Dworkin (1977), particularly 14-130; Habermas (1996); Rawls (1999a); for a critical perspective, see Hart (1958).

[125] See §§ 513, 655e of the German Civil Code (BGB).

[126] See §§ 107 et seq. BGB.

[127] See §§ 1896 et seq. BGB: legal custodianship.

[128] See Hacker (2016c).

same conclusion holds if the dangers from exploitative contracts are mitigated for those most vulnerable to exploitation. If stronger privacy protection is implemented by default for those particularly valuing privacy, this expresses a commitment to protecting privacy where it is valued most. Or, conversely, if the usury ceiling (the maximum rate of interest chargeable before a loan becomes usurious) is raised for highly rational parties, this conveys the idea that freedom of contract should be strengthened where people are thought to be in a position to make smart decisions. Therefore, with personalized law, law's expressivity merely changes location; it migrates from the concrete instantiations of laws governing specific citizens to the general rules of personalization that establish, in the abstract, what legal consequences are triggered by certain scores in a number of metrics.

4.3.2 Democratic Discourse

It is possible to point to a second transformation: the mechanization and technicization of the law, possibly to the detriment of its open discursivity. The fear is that if, in the end, algorithms, empirical studies, and statistical correlations drive large parts of the content of the law, this invites technocratic rulemaking, a tendency that can already be witnessed in highly specialized, data-driven legal fields such as securities regulation or parts of (behavioral) law and economics.[129] This is not to say that the empirical turn in the law cannot have large benefits in particular instances.[130] However, one should note that data-driven personalization will necessarily change the discursive structure of the law and might lead away from a publicly channeled and generated discursivity toward a more exclusive and hermetic culture of communication in which only those are given a voice who dispose of the necessary technical know-how.

However, technological, expert-driven rule-making is not likely to decrease in the near future. As ever more technology becomes available for lawmaking, and is perceived as a better fit to the highly complex regulatory challenges of contemporary private law, the "more technological approach"[131] seems, in substantial parts of private law, necessary and inevitable.[132] As a result, democratic discourse must open itself to technological issues and, conversely, seemingly hermetic practices of coding and technological governance must open themselves to democratic oversight. The challenge is to establish a robust discourse on the normative values underlying,

[129] See, e.g., Committee of Wise Men (2001), 20 et seq., particularly Levels 2 and 3; JRC (2016); cf. further, for a critique, Bucchi (2009); Habermas (2015).

[130] See, e.g., Hamann (2014); Hacker (2017).

[131] See, e.g., Podszun (2015).

[132] But see for an argument for a return to broad rules and standards, and against expert-driven lawmaking, as a consequence of the application of complexity theory to the regulation of digital finance, and in particular cryptocurrencies, Hacker (2016d).

and expressed in, code.[133] As scholars have often noted,[134] ultimately, the ways data is collected, assembled, and screened, the ways algorithms are constructed, trained, and applied, and finally the ways results are generated, interpreted, and used, are all human decisions subject to normative evaluations and in need of public scrutiny. This holds all the more true when digital technologies are used for the purposes of lawmaking. It is not impossible to achieve. Core values of our legal system can be brought to bear on algorithmic lawmaking, by expanding, for example, the list of principles of data processing contained in Article 5 GDPR. It should include an adherence to principles of non-discrimination, non-exploitation, and adequate protection of weak and vulnerable parties, as well as respect for the real capacities of data subjects. Such principles of algorithmic lawmaking, which can guide the personalization of law from its most abstract to more concrete levels of implementation, can be fruitfully discussed in non-technical terms with lay discourse participants.

Therefore, the technical nature of personalized law should not be understood as an invitation to purely expert-driven lawmaking outside wider public scrutiny. Rather, as more and more decisions are taken by algorithms, it is time for democratic discourse to tackle the core problems inherent in this approach, and to debate a list of principles that algorithmic lawmaking must adhere to.

5 The Scope of Personalized Law: A Normative Approach

Perhaps the most important upshot of the preceding discussion of the various challenges to the legitimacy of personalized law is the insight that it is not a cure that can be universally deployed. Rather, in every instance of personalization, the benefits must be balanced against the cost. However, for all of its potential, personalization entails a number of particular disadvantages that do not lend themselves to easy quantification: the potential for abuse over time; privacy implications; and a technicization of democratic discourse which should be, but is not yet fully, answered by expanding public debate and scrutiny to the collection of data and the construction of algorithms. Therefore, a normative approach is necessary to determine where, and whether, to personalize law. I submit that benefits will often be greater than costs in cases in which the three challenges described in the first part are most virulent: lack of awareness concerning fundamental threats to privacy by the use of "free" online services (Facebook, Google); exploitative contracting in, e.g., cell phone and credit card markets[135]; or discrimination by algorithm on platforms

[133] Cf. also Graber (2016), 21-23 (discussing meta-rules for code, expressing societal values, in the realm of personalized internet content engendered by data-processing companies such as Google, Facebook or Amazon).

[134] Silver (2012), 9: "The numbers have no way of speaking for themselves. We speak for them. We imbue them with meaning"; Citron / Pasquale (2014), 4.

[135] Shui / Ausubel (2005); Grubb (2009, 2015); Calo (2014).

providing access to essential goods such as housing or labor.[136] In all of these cases, actors vary by their degree of awareness, or proneness to exploitation and discrimination. Personalized law can offer specific remedies here. However, its application should follow a number of guidelines in order to meet the challenges outlined in the previous sections.

First and foremost, a necessary condition for personalization is that legal equality be strengthened, not undermined. Therefore, only metrics that uncover significant differences between persons and that are directly relevant to the purpose of the provision may be used. Furthermore, a normative approach involves decisions about the mandatory or default nature of personalization, about the metrics used, and about a government-based or a company-based storage and processing of data. Mandatory personalization should be reserved for cases of significant negative externalities imposed by specific actors, which can be matched with greater duties to internalize these costs (see, for example, the suggestion by Omri Ben-Shahar and Ariel Porat to personalize negligence law[137]). Otherwise, a default regime should be employed so that, depending on the circumstances, people can opt into or opt out of personalized law. An opt-in system should be favored when particularly sensitive data is used by the government.[138] An opt-out system is more appropriate where data is already lawfully processed by companies and would be matched with specific duties of the companies vis-à-vis their clients. Generally, wherever possible, less sensitive metrics should be favored over more intrusive ones, so as to minimize privacy concerns.

For a company-based system of personalization only legally acquired data may be used. It must be matched with a monitoring system to ensure that the data used is not selectively collected and processed.[139] If such an enforcement mechanism is successfully deployed, company-based personalization offers the advantage of keeping data away from governments, mitigating the potential for abuse by state authorities. Furthermore, it promises to end the unilateral use of Big Data for the benefit of those in possession of data and algorithms by using Big Data for the very benefit of data subjects.

In a government-based system of personalization, metrics that are less privacy-sensitive should be used. This, for example, should rule out information on personality traits.[140] Furthermore, in cases in which it can be assumed that counterparties already have the data, it is best to resort to government-based personalization, as here individual scores have to be communicated to counterparties.

The exact implementation of personalized law must be decided on a case-by-case basis. However, the preceding discussion should offer some guidelines for the design and scope of personalization. Most importantly, despite its technological hue, the data-driven tailoring of laws is not exempt from normative considerations.

---

[136] See, e.g., Barocas / Selbst (2016); Kim (2017).

[137] Ben-Shahar / Porat (2016).

[138] Cf. also Busch (2016), 10.

[139] For concrete proposals of such a monitoring system, see Citron / Pasquale (2014), 18-28.

[140] See op. cit. note 68 et seq.

Very much to the contrary, it will be a crucial challenge for the future of private law to formulate, and publicly debate, core principles which safeguard key values of fairness, non-discrimination, and freedom in algorithmic lawmaking.

6 Conclusion

Despite all the challenges it poses, the démarche toward a more personalized law seems rather likely, and thus a key challenge for lawmaking in market contexts. The first elements of a merger of digital technology with regulation can be found in Google's takeover of entire town administrations in the US via its 'Government Innovation Lab'.[141] The increasing interest in personalized law among scholars and policymakers testifies to its potential for envisioning, and enacting, new methods of market regulation; simultaneously, however, its development needs to be accompanied by a rigorous examination of its strengths and weaknesses.

The move toward a greater personalization of private law harbors a currently untapped potential for the effective design of legally instituted forms of exchange. Legal typifications that currently follow status-based approaches (consumer; retail investor) can be transformed into high-resolution categories that are tailored to specific groups or individuals and their necessities. At best, this can create liberties that have so far remained foreclosed by overinclusive mandatory law; it may serve equality where thus far the same practices have been applied to fundamentally different actors; and it can foster fairness were companies so far have unilaterally used Big Data for their own good. Ultimately, personalized law can be used to remedy the very digital market failures the use of Big Data engendered in the first place. By singling out those individuals most likely to suffer from market failures in data-driven markets, regulation may remedy these failures where necessary while at the same time maintaining freedom of contract, and innovation, to a greater extent for those able to fend for themselves.

Simultaneously, however, personalization triggers a host of new problems. The technical difficulties of obtaining and analyzing data robust enough to have legal consequences attached to it will likely become smaller as technology proceeds. This chapter, however, has assessed the legitimacy of personalized law by considering three sets of challenges, posed by the positive law of data protection, by considerations of equality and justice, and finally by legal and democratic theory. To square data-driven laws with a robust understanding of data protection and privacy remains a matter of fine-tuning. In this, it is helpful to distinguish two types of personalization: government-based and company-based. In the former case a government agency collects and analyzes the data, and personalizes law accordingly. In the latter case, companies are required by law to use the data they lawfully collect not only for their own benefit but also for the benefit of the individual client. While this form of personalization does not add any significant novel concerns about privacy beyond

[141] Lobe (2015).

the problems posed by company profiling at the moment, government-based personalization is prone to exacerbate privacy concerns and to open the door to abuse of data by authoritarian or malevolent regimes. Therefore, personalization primarily undertaken by government agencies should refrain from using highly sensitive metrics (such as personality trait information) and should generally be based on an optional regime, unless significant negative externalities justify mandatory personalization.

A second challenge to the legitimacy of personalized law stems from considerations of equality and justice. In private law, two concepts of equality are employed by scholars and courts. The first, more limited concept refers to an equality of sanctions and compensation: it postulates that remedies (such as damages) generally should apply irrespective of a person's standing, wealth or other personal characteristics. However, outside of private law, this rule already has some exceptions, for example in income-based criminal day fines, which apply in many European countries, and personalized law promises to further adapt the severity of sanctions to individual levels of tolerance. Thus, not the amount of the sanction itself, but its effect on the person is rendered more equal between citizens. More importantly, however, the CJEU, national constitutional courts, and most legal scholars operate with a second concept of equality in all other domains, which is based on the idea that similar situations should be treated similarly and different ones differently. This principle asks us to put forward adequate reasons for distinguishing one class of situations, or persons, from another in the context of specific norms. Here, personalization may even be required to serve equality if it helps to uncover legally relevant differences between persons: to treat persons in the same way when a law has vastly different effects on them does not further, but rather undermines, such a concept of legal equality.

A third challenge arises from considerations of legal and democratic theory where the expressive function of the law and its open discursivity come under increasing pressure. However, law's expressivity can be recovered in personalized law in the deeply normative decisions behind the general allocations of legal consequences to abstract personal characteristics. Such allocations may serve a variety of normative goals, and their concrete instantiation will be an expression of values that go beyond the immediate effect of the law. For example, if particularly vulnerable groups are specifically protected against discrimination by algorithm, this is simultaneously a sign that our society will not tolerate discrimination. Conversely, this points to a crucial challenge for democratic discourse, which has yet to tackle the normative decisions underlying the construction of algorithms and the interpretation of their results. A normative approach to personalization should make these fault lines visible and point to the necessary trade-offs, for example between privacy and the purpose of certain laws, which market regulation will have to deal with in the future. Therefore, what has to be developed is a normative account of the use of algorithms in regulation, and of the ways in which fundamental societal values can be implemented in and furthered by code. Only such critical reflection will render algorithm-driven laws legitimate, discursively open-ended, and controllable by public institutions.

References

Acquisti, A. / Brandimarte, L. / Hancock, J. (2015), Online Self-Disclosure and Offline Threat Detection, available at: www.econinfosec.org/archive/weis2015/papers/WEIS_2015_acquisti.pdf

Adler, M. (2000), Expressive Theories of Law: A Skeptical Overview, 148 University of Pennsylvania Law Review 1363

Ágh, A. (2015), De-europeanization and de-democratization trends in ECE: from the Potemkin democracy to the elected autocracy in Hungary, 8 (2) Journal of Comparative Politics 4

Allen, R. (2007), Article 13 EC, evolution and current contexts, in: H. Meenan (Ed.), Equality Law in an Enlarged European Union, 38, Cambridge University Press

Anderson, E.S. / Pildes, R.H. (2000), Expressive Theories of Law: A General Restatement, 148 University of Pennsylvania Law Review 1503

Aristotle, Nicomachean Ethics (H. Rackham, trans.), (2014), Loeb Classical Library 73, Harvard University Press

Aristotle, Politics (H. Rackham, trans.), (2014) Loeb Classical Library 264, Harvard University Press

Ayres, I. / Schwartz, A. (2014), The No-Reading Problem in Consumer Contract Law, 66 Stanford Law Review 545

Back, M. / Stopfer, J. / Vazire, S. / Gaddis, S. / Schmukle, S. / Egloff, B. / Gosling, S. (2010), Facebook Profiles Reflect Actual Personality, Not Self-Idealization, 21 Psychological Science 372

Bakos, Y. / Marotta-Wurgler, F. / Trossen, D.R. (2014), Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts, 43 The Journal of Legal Studies 1

Bar-Gill, O. (2012), Seduction by Contract, Oxford University Press

Barocas, S. / Selbst, A. (2016), Big Data's Disparate Impact, 104 California Law Review 671

Barrick, M.R. / Mount, M.K. (1991), The Big Five Personality Dimensions and Job Performance: A Meta-Analysis, 44 Personnel Psychology 1

Becker, S.O. / Fetzer, Th. / Novy, D. (2016), Who Voted for Brexit? A Comprehensive District-Level Analysis, CAGE Working Paper 305 (October 2016), available at: http://www2.warwick.ac.uk/fac/soc/economics/research/centres/cage/publications/workingpapers/

Ben-Shahar, O. / Chilton, A.S. (2016), Simplification of Privacy Disclosures: An Experimental Test, University of Chicago Coase-Sandor Institute for Law & Economics Research Paper No. 737 (13 April 2016), available at: http://ssrn.com/abstract=2711474

Ben-Shahar, O. / Porat, A. (2016), Personalizing Negligence Law, New York University Law Review (forthcoming), University of Chicago Coase-Sandor Institute for Law & Economics Research Paper No. 731, available at: http://ssrn.com/abstract=2654458

Block, J. (1995), A contrarian view of the five-factor approach to personality description, 117 Psychological Bulletin 187

Bourguignon, F. (2015), The Globalization of Inequality (Thomas Scott-Railton, trans.), Princeton University Press

Brynjolfsson, E. / McAffee, A. (2014), The Second Machine Age. Work, Progress, and Prosperity in a Time of Brilliant Technologies, W.W. Norton & Co

Bucchi, A. (2009), Beyond Technocracy. Science, Politics and Citizens (Adrian Belton, trans.), Springer

Busch, Ch. (2016), The Future of Pre-Contractual Information Duties: From Behavioural Insights to Big Data, in: Ch. Twigg-Flesner (Ed.), Research Handbook on EU Consumer and Contract Law, Edward Elgar (forthcoming), available at: http://ssrn.com/abstract=2728315

Calders, T. / Verwer, S. (2010), Three Naïve Bayes Approaches for Discrimination-Free Classification, 21 Data Mining and Knowledge Discovery 277

Calders, T. / Žliobaitė, I. (2013), Why Unbiased Computational Processes Can Lead to Discriminative Decision Procedures, in: B. Custers / T. Calders / B. Schermer / T. Zarsky (Eds.), Discrimination and Privacy in the Information Society, 43, Springer

Calo, R. (2014), Digital Market Manipulation, 82 George Washington Law Review 995
Cancik, H. (1998), Gleichheit und Freiheit. Die antiken Grundlagen der Menschenrechte, in: id., Antik — Modern. Beiträge zur römischen und deutschen Kulturgeschichte, 293, Metzler
Caracciolo di Torella, E. / Masselot, A. (2004), The Future of Sex Equality, in: T. Tridimas / P. Nebbia (Eds.), 2 European Union Law for the Twenty-First Century 333, Hart
Carney, D.R. / Jost, J.T. / Gosling, S.D. / Potter, J. (2008), The Secret Lives of Liberals and Conservatives: Personality Profiles, Interaction Styles, and the Things They Leave Behind, 29 Political Psychology 807
Chittaranjan, G. / Blom, J. / Gatica-Perez, D. (2013), Mining large-scale smartphone data for personality traits, 17 Personal and Ubiquitous Computing 433
Citron, D. / Pasquale, F. (2014), The Scored Society: Due Process for Automated Predictions, 89 Washington Law Review 1
Colonna, L. (2013), A Taxonomy and Classification of Data Mining, 16 SMU Science and Technology Law Review 309
Cormen, T.H. / Leiserson, Ch.E. / Rivest, R.L. / Stein, C. (2009), Introduction to Algorithms, 3rd ed., MIT Press
Deslauriers, M. (2013), Political unity and inequality, in: M. Deslauriers / P. Destrée (Eds.), The Cambridge Companion to Aristotle's Politics, 117, Cambridge University Press
Donohue, J. (1989), Prohibiting Sex Discrimination in the Workplace: An Economic Perspective, 56 University of Chicago Law Review 1337
Dou, Y. / Niculescu, M.F. / Wu, D.J. (2013), Engineering Optimal Network Effects via Social Media Features and Seeding in Markets for Digital Goods and Services, 24 Information Systems Research 164
Dworkin, R. (1977), Taking Rights Seriously, Harvard University Press
Edelman, B.G. / Luca, M. / Svirsky, D. (2016), Racial Discrimination in the Sharing Economy: Evidence from a Field Experiment, American Economic Journal: Applied Economics (forthcoming), available at: http://ssrn.com/abstract=2701902
Evans S. / Schmalensee, R. (2015), The Antitrust Analysis of Multi-Sided Platform Businesses, in: R.D. Blair / D.D. Sokol (Eds.), 1 Oxford Handbook of International Antitrust Economics 407, Oxford University Press
Feldman, Y. / Lobel, O. (2015), Behavioral Tradeoffs: Beyond the Land of Nudges Spans the World of Law and Psychology, in: A. Alemanno / A.-L. Sibony (Eds.), Nudge and the Law: A European Perspective on Behavioural Policymaking, 301, Hart
Fleischacker, S. (2004), A Short History of Distributive Justice, Harvard University Press
Fomina, J. / Kucharczyk, J. (2016), Populism and Protest in Poland, 27 Journal of Democracy 58
Franceschi-Bicchierai, L. (2016), Who Hacked Sony Pictures? Two Years Later, No One's Really Sure, Motherboard (12 July 2016), available at: https://motherboard.vice.com/read/who-hacked-sony-pictures-two-years-later-no-ones-really-sure
Frank, R.H. / Cook, P.J. (1995), The Winner-Take-All Society, The Free Press
Gandomi, A. / Haider, M. (2015), Beyond the hype: Big data concepts, methods, and analytics, 35 International Journal of Information Management 137
Goldfarb, A. / Greenstein, S.M. / Tucker, C.E. (2015): Economic Analysis of the Digital Economy, The University of Chicago Press
Gordon, R.J. (2016), The Rise and Fall of American Growth: The US Standard of Living Since the Civil War, Princeton University Press
Gosling, S. / Rentfrow, P. / Swann Jr., W. (2003), A very brief measure of the Big-Five personality domains, 37 Journal of Research in Personality 504
Graber, Ch. B. (2016), The Future of Online Content Personalisation: Technology, Law and Digital Freedoms, i-call Working Paper No. 01 (3 October 2016), available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2847008
Grubb, M.D. (2009), Selling to Overconfident Consumers, 99 American Economic Review 1770
Grubb, M.D. (2015), Overconfident Consumers in the Marketplace, 29 Journal of Economic Perspectives 9

Grünberger, Michael (2013), Personale Gleichheit. Der Grundsatz der Gleichbehandlung im Zivilrecht, Nomos
Habermas, J. (1996), Between Facts and Norms (William Rehg trans.), MIT Press
Habermas, J. (2015), The Lure of Technocracy (Ciaran Cronin trans.), Polity
Hacker (2016a), Nudge 2.0 – The Future of Behavioral Analysis of Law, in Europe and beyond, 24 European Review of Private Law 297
Hacker, P. (2016b), One Size Fits All? Heterogeneity and the Enforcement of Consumer Rights in the EU after Faber, Case Note on the Judgment of the Court (First Chamber) of 4 June 2015, Froukje Faber v Autobedrijf Hazet Ochten BV (C-497/13), 12 European Review of Contract Law 167
Hacker, P. (2016c), Personalizing EU Private Law. From Disclosures to Nudges and Mandates, European Review of Private Law (forthcoming).
Hacker, P. (2016d), Chaos, Complexity, and Cryptocurrencies. Some Prospects for the Regulation of the New Financial Order, Working Paper (on file with author)
Hacker, P. (2017), Verhaltensökonomik und Normativität. Die Grenzen des Informationsmodells im Privatrecht und seine Alternativen, Mohr Siebeck (forthcoming)
Hacker, P. / Dimitropoulos, G. (2017), Behavioural Law & Economics and Sustainable Regulation: From Markets to Learning Nudges, in: K. Mathis / B.R. Huber (Eds.), Environmental Law and Economics, 155, Springer
Hacker, P. / Petkova, B. (2016), Reining in the Big Promise of Big Data. Transparency, Inequality, and New Regulatory Frontiers, Northwestern Journal of Technology and Intellectual Property (forthcoming), available at: http://ssrn.com/abstract=2773527
Hamann, H. (2014), Evidenzbasierte Jurisprudenz. Methoden empirischer Forschung und ihr Erkenntniswert für das Recht am Beispiel des Gesellschaftsrechts, Mohr Siebeck
Hart, H.L.A. (1958), Positivism and the Separation of Law and Morals, 71 Harvard Law Review 593
Heidhues, P. / Kőszegi, B. (2010), Exploiting Naïvete about Self-Control in the Credit Market, 100 American Economic Review 2279
Heidhues, P. / Kőszegi, B. / Murooka, T. (2012), Inferior Products and Profitable Deception, Working Paper (2012), available at: https://www.esmt.org/inferior-products-and-profitable-deception
Jaumotte, F. / Lall, S. / Papageorgiou, Ch. (2013), Rising Income Inequality: Technology, or Trade and Financial Globalization?, 61 IMF Economic Review 271
Jansen, N. (2005), Konturen eines europäischen Schadensrechts, Juristenzeitung 160
John, O.P. / Srivastava, S. (1999), The Big Five trait taxonomy: History, measurement, and theoretical perspectives, in: L.A. Pervin / O.P. John (Eds.), Handbook of Personality: Theory and Research, 102, 2nd ed., The Guilford Press
Judis, J. (2016), The Populist Explosion. How the Great Recession Transformed American and European Politics, Columbia Global Reports
Kantorowicz-Reznichenko, E. (2015), Day-Fines: Should the Rich Pay More?, 11 Review of Law and Economics 481
Kamenica, E. / Mullainathan, S. / Thaler, R. (2011), Helping Consumers Know Themselves, 101 American Economic Review: Papers and Proceedings 417
Kant, I. (1785), Grundlegung zur Metaphysik der Sitten, in: Kant's gesammelte Schriften, hg. von der Königlich Preußischen Akademie der Wissenschaften, Erste Abteilung: Kant's Werke, Band IV, 385, Berlin 1911
Kim, P.T. (2017): Data-Driven Discrimination at Work, William and Mary Law Review (forthcoming), available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2801251
Kirchhof, P. (2015), Kommentar, in: Maunz/Dürig, Grundgesetz-Kommentar, 75. EL 2015, Art. 3
Kőszegi, B. (2014), Behavioral Contract Theory, 52 Journal of Economic Literature 1075
Kymlicka, W. (2002), Contemporary Political Philosophy, 2nd ed., Oxford University Press
Lowry, S. / Macpherson, G. (1988), A Blot on the Profession, 296 British Medical Journal 657

MacDonald, D.A. (2007), Viewpoint: Card Industry Questions Congress Needs to Ask [sic], American Banker (23 March 2007), available at: http://www.americanbanker.com/issues/172_58/-306775-1.html
Madden, M. / Rainie, L. (2015), Americans' Attitudes About Privacy, Security and Surveillance, Pew Research Center (20 May 2015), available at: http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/
McCaffery, E.J. (1993), Slouching Towards Equality: Gender Discrimination, Market Efficiency, and Social Change, 103 Yale Law Journal 595
McCrae, R. / John, O. (1992), An introduction to the five-factor model and its applications, 60 Journal of Personality 175
Meenan, H. (2007), Introduction, in: id. (Ed.), Equality Law in an Enlarged European Union, 3, Cambridge University Press
Miller, D. (2003), Political Philosophy. A Very Short Introduction, Oxford University Press
Oetker, H. (2016), Kommentar, in: Münchener Kommentar zum BGB, 7th ed., § 249, C.H. Beck
Pasquale, F. (2015), The Black Box Society. The Secret Algorithms That Control Money and Information, Harvard University Press
Piketty, Th. (2014), Capital in the Twenty-First Century (Arthur Goldhammer trans.), The Belknap Press of Harvard University Press
Porat, A. / Strahilevitz, L.J. (2014), Personalizing Default Rules and Disclosure with Big Data, 112 Michigan Law Review 1417
Podszun, R. (2015), The More Technological Approach: Competition Law in the Digital Economy, in: G. Surblyte (Ed.), Competiton on the Internet, 101, Springer
Pöschl, M. (2008), Gleichheit vor dem Gesetz, Springer
Pojman, L.P. / Westmoreland, R. (1997), Introduction: The Nature and Value of Equality, in: id. (Eds.), Equality, 1, Oxford University Press
Posner, Richard A. (2014), Economic Analysis of Law, 9th ed., Wolters Kluwer
Rawls, J. (1974), Some Reasons for the Maximin Criterion, 64 American Economic Review: Papers and Proceedings 141
Rawls, J. (1999a), A Theory of Justice, revised ed., Harvard University Press
Rawls, J. (1999b), Distributive Justice, in: id., 130, Collected Papers, edited by Samuel Friedman, Harvard University Press
Rawls, J. (2001), Justice as Fairness. A Restatement, The Belknap Press of Harvard University Press
Rosenblat, A. / Levy, K. / Barocas, S. / Hwang, T. (2016), Discriminating Tastes: Customer Ratings as Vehicles for Bias, Intelligence and Autonomy (October 2016), available at: http://autonomy.datasociety.net
Saez, E. / Zucman, G. (2016), Wealth Inequality in the United States since 1913: Evidence from Capitalized Income Tax Data, 131 Quarterly Journal of Economics 519
Samuelson, W. / Zeckhauser, R. (1988), Status Quo Bias in Decision Making, 1 Journal of Risk and Uncertainty 7
Schwartz, A. (2015), Regulating for Rationality, 67 Stanford Law Review 1373
Schwartz, A. / Wilde, L.L. (1979), Intervening in Markets on the Basis of Imperfect Information: A Legal and Economic Analysis, 127 University of Pennsylvania Law Review 630
Sen, A. (1980), Equality of What?, in: S. McMurrin (Ed.): The Tanner Lectures on Human Values, 185, Cambridge University Press
Sen, A. (2009), The Idea of Justice, The Belknap Press of Harvard University Press
Silver, N. (2012): The Signal and the Noise. Why So Many Predictions Fail – but Some Don't, Penguin Press
Smith, N. (2011), Basic Equality and Discrimination. Reconciling Theory and Law, Ashgate
Staiano, J. / Lepri, B. / Aharony, N. / Pianesi, F. / Sebe, N. / Pentland, A. (2012), Friends don't Lie – Inferring Personality Traits from Social Network Structure, Proceedings of the 2012 ACM Conference on Ubiquitous Computing – UbiComp '12, 321, available at: https://doi.org/10.1145/2370216.2370266

Stanovich, K.E. / West, R.F. (2000), Individual differences in reasoning: Implications for the rationality debate?, 23 Behavioral and Brain Sciences 645
Stiglitz, J. (2000), The Contributions of the Economics of Information to Twentieth Century Economics, 115 Quarterly Journal of Economics 141
Stolleis, M. (2003): Historische und ideengeschichtliche Entwicklung des Gleichheitsgrundsatzes, in: R. Wolfrum (Ed.), Gleichheit und Nichtdiskriminierung im nationalen und internationalen Menschenrechtsschutz, 7, Springer
Sunstein, C. (1991), Why Markets Don't Stop Discrimination, 8 Social Philosophy and Policy 22
Sunstein, C. (1996), On the Expressive Function of Law, 144 University of Pennsylvania Law Review 2021
Sunstein, C. (2013), Impersonal Default Rules vs. Active Choices vs. Personalized Default Rules: A Triptych, Working Paper (19 May 2013), available at: http://ssrn.com/abstract=2171343
Sweeney, L. (2013), Discrimination in Online Ad Delivery, 56 Communications of the ACM 44
Tene, O. / Polonetsky, J. (2012), Privacy in the Age of Big Data: A Time for Big Decisions, 64 Stanford Law Review Online 63
Tridimas, T. (2006), The General Principles of EU Law, 2nd ed., Oxford University Press
Tutt, A. (2016), An FDA for Algorithms, Working Paper (15 March 2016), available at: http://ssrn.com/abstract=2747994
Westen, P. (1982), The Empty Idea of Equality, 95 Harvard Law Review 537
Waldron, J. (1991), The Substance of Equality, 89 Michigan Law Review 1350
Wieacker, F. (1967), Privatrechtsgeschichte der Neuzeit, 2nd ed., Vandenhoeck & Ruprecht
Wiggins, J.S. / Pincus, A.L. (1989), Conceptions of Personality Disorders and Dimensions of Personality, 1 Psychological Assessment: A Journal of Consulting and Clinical Psychology 305
Willis, L. (2013), When Nudges Fail: Slippery Defaults, 80 University of Chicago Law Review 1155

Additional Sources

CMA (2016), Retail banking market investigation, Final Report (9 August 2016), available at: https://www.gov.uk/cma-cases/review-of-banking-for-small-and-medium-sized-businesses-smes-in-the-uk
Committee of Wise Men (2001), Final Report of the Committee of Wise Men on the Regulation of European Securities Markets (15 February 2001), available at: http://ec.europa.eu/internal_market/securities/docs/lamfalussy/wisemen/final-report-wise-men_en.pdf
Grasegger, H. / Krogerus, M. (2016), Ich habe nur gezeigt, dass es die Bombe gibt, Das Magazin of 3 December 2016, available at: https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/
IDC, Press Release, Worldwide Big Data and Business Analytics Revenues Forecast to Reach $187 Billion in 2019, According to IDC, 23 May 2016, available at: https://www.idc.com/getdoc.jsp?containerId=prUS41306516
Janisch, W. / Ulrich, S. (2016), Die EU muss klar Position beziehen, Süddeutsche Zeitung of 21 October 2016, available at: http://www.sueddeutsche.de/politik/verfassungsrichter-vosskuhle-und-fabius-die-eu-muss-klar-position-beziehen-1.3215934
JRC (2016), Behavioural Insights Applied to Policy, European Report 2016, available at: https://ec.europa.eu/jrc/en/event/conference/biap-2016
Karpf, D. (2017), Will the Real Psychometric Targeters Please Stand Up?, Civicist of 1 February 2017, available at: http://civichall.org/civicist/will-the-real-psychometric-targeters-please-stand-up
Lobe, A. (2015), Google will den Staat neu programmieren, Frankfurter Allgemeine Zeitung of 14 October 2015, available at: http://www.faz.net/aktuell/feuilleton/medien/google-gruendet-in-den-usa-government-innovaton-lab-13852715.html

Perlroth, N. (2016), Yahoo Says Hackers Stole Data on 500 Million Users in 2014, New York Times of 22 September 2016, available at: http://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html

Pew Research Center (2014), Public Perceptions of Privacy and Security in the Post-Snowden Era, Report (12 November 2014), available at: http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/

PYMNTS (2016), Hacked Uber Accounts Trump Credit Cards On Dark Web, PYMNTS.com (21 January 2016), available at: http://www.pymnts.com/news/security-and-risk/2016/hacked-uber-accounts-trump-credit-cards-on-dark-web

Schwindt, O. (2016), Celebrity Nudes to Credit Cards: 9 Big Hack Attacks, The Wrap of 23 September 2016, available at: http://www.thewrap.com/celebrity-nudes-to-credit-cards-9-biggest-hack-attacks-photos/3/

Shui, H. / Ausubel, L. (2005), Time Inconsistency in the Credit Card Market, unpublished manuscript (30 January 2005), available at: http://web.natur.cuni.cz/~houdek3/papers/economics_psychology/Shui%20Ausubel%202006.pdf

Part II
Personal Data and Competition Law

Blurring Boundaries of Consumer Welfare

How to Create Synergies Between Competition, Consumer and Data Protection Law in Digital Markets

Inge Graef

Contents

1 Introduction ... 122
2 Interaction of Competition, Consumer and Data Protection Law ... 123
2.1 Competition Law ... 123
2.2 Consumer Protection Law ... 126
2.3 Data Protection Law ... 128
2.4 Findings ... 131
3 Enforcement of Data Portability ... 132
3.1 Competition Law Angle of Data Portability ... 132
3.2 Comparing Data Protection and Competition Law ... 134
3.3 Possible Role of Consumer Protection Law ... 135
4 Assessing Exploitative Abuse Under Article 102 TFEU ... 137
4.1 Excessive Pricing ... 137
4.2 Benchmarks from Data and Consumer Protection Law ... 138
5 Potential Role of Data Protection and Consumer Law Considerations in Merger Review ... 141
5.1 Current Reluctance of the Commission and the Court of Justice ... 141
5.2 Consumer and Data Protection as Legitimate Interests Under Merger Review ... 144
5.3 Illustrations of Data Protection-Related Merger Remedies ... 146
6 Conclusion ... 148
References ... 149

Abstract The boundaries between the fields of competition, consumer and data protection law have become blurred in the digital economy. This is particularly the case for the rules governing practices of market players relating to the collection and use of personal data of individuals. In addition to possible competition issues, concerns are increasingly raised about the level of data and consumer protection offered by current market players. Ongoing policy and academic debates have begun to

Assistant Professor at the Tilburg Institute for Law, Technology, and Society (TILT) and the Tilburg Law and Economics Center (TILEC).

I. Graef (✉)
Tilburg Law School, Tilburg, Netherlands
e-mail: i.graef@tilburguniversity.edu

M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law*, MPI Studies on Intellectual Property and Competition Law 28, https://doi.org/10.1007/978-3-662-57646-5_6

consider the question of how these three legal fields interact. The chapter aims to shed light on this issue by comparing the relevant legal concepts as well as the available remedies in each of these areas of law and by outlining how synergies can be achieved with the objective of providing consumers in digital markets with a more integrated form of protection.

1 Introduction

The rise of the digital economy has increased the need for different legal fields to work together to provide individuals with an adequate level of protection. Reference can in particular be made to the increasing collection and use of personal data from individuals by market players. Although online services such as search and social networking are commonly offered free of charge, providers instead gather information about the profile and behaviour of individuals in exchange for being able to use the search or social networking functionalities. This information is monetised by letting advertisers target specific groups of individuals defined on the basis of the collected data. The data is also a vital input for providing services of good quality to consumers in the form of, for example, relevant and personalised search results or social network interactions. As a result, user data is becoming an asset to which undertakings need access in order to viably compete in digital markets. From this perspective, data may form a source of market power and trigger the application of the competition rules.[1] In addition, concerns have been raised about the level of consumer and data protection by current market players. The European Data Protection Supervisor[2] has been particularly active in this area after the publication of its Preliminary Opinion on 'Privacy and competitiveness in the age of big data'[3] in March 2014, which outlines how the fields of data protection, competition law and consumer protection intersect in the digital economy. In September 2016, the European Data Protection Supervisor made several concrete recommendations in its Opinion on 'coherent enforcement of fundamental rights in the age of big data', including the setting up of a so-called digital clearing house, to consist of a voluntary network of regulatory bodies to share information about possible abuses in the digital environment.[4]

Against this background, the chapter expands on this ongoing debate by considering the relationship between competition, consumer and data protection law in digital markets, which are built on the collection and processing of personal data (Sect. 2). Afterwards, three areas are identified which would benefit from synergies

[1] See also Graef (2015a).

[2] The European Data Protection Supervisor is the independent supervisory authority that oversees the data-processing activities of the EU institutions and provides the EU institutions with advice on data protection issues.

[3] European Data Protection Supervisor (2014).

[4] European Data Protection Supervisor (2016).

between these three legal fields: the enforcement of data portability (Sect. 3); the assessment of exploitative abuse under Article 102 TFEU (Sect. 4); and the potential role of data protection and consumer considerations in merger review (Sect. 5).[5]

2 Interaction of Competition, Consumer and Data Protection Law

EU competition, consumer and data protection law share common goals. These three legal fields aim to protect the general public (either consumers more generally under competition law or individual consumers and data subjects under consumer and data protection law, respectively) and to contribute to the functioning of the internal market. However, the means by which these objectives are pursued differ.

2.1 Competition Law

Protocol No. 27 on the internal market and competition, as annexed to the Lisbon Treaty, makes clear that the internal market that the European Union is to establish in accordance with Article 3(3) of the Treaty on European Union includes '*a system ensuring that competition is not distorted*'.[6] As regards the objectives of the field, the Court of Justice stated in *TeliaSonera* that the EU competition rules are necessary for the functioning of the internal market and seek '*to prevent competition from being distorted to the detriment of the public interest, individual undertakings and consumers, thereby ensuring the well-being of the European Union*'.[7] To this end, competition law tries to enhance consumer welfare by intervening against restrictive practices, abusive behaviour and concentrations that significantly impede effective competition.

Article 101(1) of the Treaty on the Functioning of the European Union (TFEU) prohibits agreements between undertakings, decisions by associations of undertakings and concerted practices which may affect trade between Member States and which have as their object or effect the prevention, restriction or distortion of competition within the internal market. This prohibition does not apply when the cumulative conditions of Article 101(3) TFEU are met. These conditions require that the restrictive practice at issue: (1) contributes to improving the production or distribution of goods or to promoting technical or economic progress; (2) allows consumers a fair share of the resulting benefit; (3) does not impose on the undertakings concerned restrictions which are not indispensable to the attainment of these objectives;

[5] The analysis in this chapter builds upon earlier work in Graef (2016), where a more elaborate and detailed discussion of these and related issues can be found, in particular on p. 325-363.

[6] Protocol (No 27) on the internal market and competition [2012] OJ C 326/309.

[7] ECJ, Konkurrensverket v. TeliaSonera Sverige AB, C-52/09, ECLI:EU:C:2011:83, para. 22.

and (4) does not afford such undertakings the possibility of eliminating competition in respect of a substantial part of the products in question.

Article 102 TFEU contains the prohibition on abuse of dominance, banning as incompatible with the internal market any abuse by one or more undertakings with a dominant position in so far as it may affect trade between Member States. A distinction is commonly made between exclusionary abuse by which a dominant undertaking excludes competitors from the market and exploitative abuse by which a dominant undertaking exploits suppliers or customers. Although Article 102 TFEU does not have a provision like paragraph 3 of Article 101 TFEU, which renders the prohibition on abuse of dominance inapplicable when certain conditions are fulfilled, it is clear that abusive conduct can also be justified. In the Guidance Paper on exclusionary conduct under Article 102 TFEU, the European Commission specified that a dominant undertaking may do so either by demonstrating that its conduct is objectively necessary or by demonstrating that its conduct produces substantial efficiencies which outweigh any anticompetitive effects on consumers.[8] This approach of the European Commission was endorsed by the Court of Justice in *Post Danmark I* when arguing that a dominant undertaking may justify its abusive behaviour by demonstrating '*either that its conduct is objectively necessary …, or that the exclusionary effect produced may be counterbalanced, outweighed even, by advantages in terms of efficiency that also benefit consumers*'.[9]

Merger review, in turn, takes place on the basis of the EU Merger Regulation,[10] which applies to proposed concentrations meeting the turnover thresholds to qualify as a concentration with a Community dimension.[11] Concentrations with a Community dimension have to be notified to the European Commission prior to their implementation.[12] The Commission will then decide to approve the concentration or not depending on whether it raises serious doubts as to its compatibility with the common market.[13]

Although the exact scope of protection offered by EU competition law is the subject of recurrent debate,[14] it is clear that the competition rules as currently enforced by the European Commission and the EU Courts predominantly seek to protect economic efficiency to the benefit of consumers. This implies that non-efficiency concerns relating to, for instance, media pluralism, environmental protection, public

[8] Communication from the Commission — Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings (Guidance Paper), [2009] OJ C 45/7, para. 28.

[9] ECJ, Post Danmark A/S v. Konkurrencerådet (Post Danmark I), C-209/10, ECLI:EU:C:2012:172, para. 41.

[10] Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings (EU Merger Regulation) [2004] OJ L 24/1.

[11] Article 1 of the EU Merger Regulation.

[12] Article 4 of the EU Merger Regulation.

[13] Article 6 of the EU Merger Regulation.

[14] For recent work, see for instance the contributions in Zimmer (2012). In the context of Article 101 TFEU, see Van Rompuy (2012). In the context of Article 102 TFEU, see Nazzini (2011).

health and also data protection are in principle protected through other laws and means to the extent that they cannot be translated into economic efficiency benefits. In this regard and as indicated by the Commission in its *Facebook/WhatsApp* merger decision, one should note that data protection may constitute a parameter on the basis of which companies compete in a particular market.[15] In the context of the *Microsoft/LinkedIn* merger, the Commission made explicit that consumer choice in relation to privacy protection was an important parameter of competition between professional social networks which could be endangered by the merger if the market were to reach a tipping point in favour of LinkedIn.[16] In such circumstances, the notion of economic efficiency will comprise data protection. However, the issue at stake here goes beyond the possible role of data protection as a non-price parameter of competition in the standard competition analysis. The point to be discussed is whether competition law should be used as an instrument to stimulate a higher level of data protection.

In this context, data protection advocates point to the focus on the protection of consumers as the main objective of EU competition law for supporting their argument that data protection considerations should be integrated into a broader consumer-welfare standard to be pursued under competition law.[17] The emphasis on the protection of consumers under the competition rules has become particularly apparent in recent judgments in the area of Article 102 TFEU. In *Post Danmark I*, the Court of Justice argued that '*Article [102 TFEU] covers not only those practices that directly cause harm to consumers but also practices that cause consumers harm through their impact on competition*'.[18] Similarly, the General Court noted in *Intel* that '*Article [102 TFEU] is aimed not only at practices which may cause damage to consumers directly, but also at those which are detrimental to them through their impact on an effective competition structure*'.[19] In *Post Danmark I*, the Court of Justice expressly stated that Article 102 TFEU does not '*seek to ensure that competitors less efficient than the undertaking with the dominant position should remain on the market*' and that '*not every exclusionary effect is necessarily detrimental to competition*'.[20] In this regard, the Court noted that '*[c]ompetition on the merits may, by definition, lead to departure from the market or the marginalisation of competitors that are less efficient and so less attractive to consumers from the point of view of, among other things, price, choice, quality or innovation*'.[21] Finally, in the Court's

[15] European Commission, Case No. COMP/M.7217 – *Facebook/WhatsApp*, 3 October 2014, para. 87.

[16] European Commission, Case No. M.8124 – *Microsoft/LinkedIn*, 6 December 2016, para. 350 and footnote 330.

[17] See for instance Kuner / Cate / Millard / Svantesson / Lynskey (2014), 247-248.

[18] ECJ, Post Danmark A/S v. Konkurrencerådet (Post Danmark I), C-209/10, ECLI:EU:C:2012:172, para. 20.

[19] GC, Intel Corp. v. European Commission, T-286/09, ECLI:EU:T:2014:547, para. 105.

[20] ECJ, Post Danmark A/S v. Konkurrencerådet (Post Danmark I), C-209/10, ECLI:EU:C:2012:172, para. 21-22.

[21] ECJ, Post Danmark A/S v. Konkurrencerådet (Post Danmark I), C-209/10, ECLI:EU:C:2012:172, para. 22.

view Article 102 TFEU '*applies, in particular, to the conduct of a dominant undertaking that, through recourse to methods different from those governing normal competition on the basis of the performance of commercial operators, has the effect, to the detriment of consumers, of hindering the maintenance of the degree of competition existing in the market or the growth of that competition*'.[22]

All these statements make clear that the main underlying goal of Article 102 TFEU as currently enforced by the EU Courts is to protect competition in order to enhance consumer welfare. As a result, a certain type of conduct which reduces competition is not necessarily abusive. What is decisive for the assessment under Article 102 TFEU is whether the reduction of competition caused by the behaviour of a dominant undertaking leads to consumer harm.[23] The key issue raised by data protection advocates such as the European Data Protection Supervisor is whether the concept of consumer harm as applied in competition enforcement may include data protection-related violations.[24]

2.2 Consumer Protection Law

EU consumer protection law aims to bring down barriers to the internal market by improving the confidence of consumers in products and services. To this end, consumer protection rules assist consumers as the weaker party in market transactions through preventing or remedying market failures. Such market failures include information inefficiencies like imperfect information, information asymmetries or bounded rationality.[25] In addition, consumer protection law is concerned with regulating social aspects of the market such as the safety and health of consumers.[26]

Several provisions in EU primary law can be distinguished that refer to consumer protection. Article 12 TFEU calls for consumer protection requirements to be taken into account in defining and implementing other Union policies and activities. In order to promote the interests of consumers and to ensure a high level of consumer protection, Article 169 TFEU requires the EU to contribute to protecting the health, safety and economic interests of consumers, as well as to promoting their right to information and education and their right to organise themselves in order to safeguard their interests. In addition, with the entry into force of the Lisbon Treaty

[22] ECJ, Post Danmark A/S v. Konkurrenceråd (Post Danmark I), C-209/10, ECLI:EU:C:2012:172, para. 24.

[23] Rousseva / Marquis (2013), 41-42.

[24] European Data Protection Supervisor (2014), para. 71: '*Given the reach and dynamic growth in online services, it may therefore be necessary to develop a concept of consumer harm, particularly through violation of rights to data protection, for competition enforcement in digital sectors of the economy*'.

[25] See for instance Cseres (2007), 129.

[26] Reference can be made here to Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety [2002] OJ L 11/4, which aims to ensure that products placed on the market are safe.

in December 2009, the Charter of Fundamental Rights of the European Union,[27] including the requirement for EU policies to ensure a high level of consumer protection as contained in Article 38, gained binding legal status.

In terms of secondary EU legislation, the consumer acquis provides for general consumer rules as well as specific rules applicable to certain sectors such as electronic communications, passenger transport, energy and financial services. With regard to EU consumer law of general application, five Directives can be distinguished.

The Consumer Rights Directive lays down, amongst other things, which information has to be provided by traders prior to the conclusion of consumer contracts.[28] This includes information about the functionality and interoperability of digital content.[29]

The Unfair Contract Terms Directive introduces the notion of 'good faith' in order to protect consumers against the use by traders of standard contract terms that are not individually negotiated and create a significant imbalance in the parties' rights and obligations to the detriment of the consumer.[30] Next to this general requirement, there is an Annex containing an indicative and non-exhaustive list of terms that may be regarded as unfair.[31] In addition, the Unfair Contract Terms Directive requires contract terms to be drafted in plain and intelligible language and states that where doubt arises about the meaning of a term, the interpretation most favourable to the consumer has to prevail.[32]

The Unfair Commercial Practices Directive protects consumers against unfair commercial practices, defined as commercial practices that are contrary to the requirements of professional diligence and materially distort or are likely to materially distort the economic behaviour of the average consumer,[33] as well as against misleading[34] and aggressive[35] commercial practices. Annex I contains a list of commercial practices which are in all circumstances considered unfair.

In turn, the Sales and Guarantees Directive[36] lays down rules on the conformity of a product with the contract and on the respective remedies.

---

[27] Charter of Fundamental Rights of the European Union [2012] OJ C 326/391.

[28] Articles 5-8 of Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights (Consumer Rights Directive) [2011] OJ L 304/64.

[29] Article 5(1)(g) and (h) and Article 6(1)(r) and (s) of the Consumer Rights Directive.

[30] Article 3(1) of the Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (Unfair Contract Terms Directive) [1993] OJ L 95/29.

[31] Article 3(3) of the Unfair Contract Terms Directive.

[32] Article 5 of the Unfair Contract Terms Directive.

[33] Article 5 of Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market (Unfair Commercial Practices Directive) [2005] OJ L 149/22.

[34] Articles 6 and 7 of the Unfair Commercial Practices Directive.

[35] Article 8 of the Unfair Commercial Practices Directive.

[36] Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees (Sales and Guarantees Directive) [1999] OJ L 171/12.

Finally, the Price Indication Directive[37] requires traders to indicate in an unambiguous, easily identifiable and clearly legible way to consumers the selling price and the unit price of a product in order to improve consumer information and to facilitate comparison of prices.

In addition to these legislative instruments that provide for substantive consumer rules, two other Directives are worth mentioning. The Misleading and Comparative Advertising Directive,[38] which applies among businesses, requires Member States to take steps to combat misleading advertising[39] and permits comparative advertising when certain conditions are met,[40] including that the advertising is objective, does not denigrate or discredit competitors' trademarks and does not create confusion among traders.

The Injunctions Directive[41] forms an important enforcement tool of EU consumer law. It requires Member States to have a court or administrative procedure in place in their national legal order for stopping infringements where collective interests of consumers protected by the Directives listed in the Annex are at stake.

Currently, all of these Directives are being evaluated by the European Commission in the context of the Regulatory Fitness and Performance Programme (REFIT), which aims to assess whether EU regulatory frameworks are still fit for purpose. In April 2018, the Commission adopted the 'New Deal for Consumers package' introducing two proposals for Directives, namely a proposal on representative actions for the protection of the collective interests of consumers repealing the Injunctions Directive and a proposal amending the Unfair Contract Terms Directive, the Unfair Commercial Practices Directive, the Price Indication Directive as well as the Consumer Rights Directive in order to improve the enforcement of consumer legislation in light of market developments brought about by the digital economy in particular.[42]

2.3 Data Protection Law

EU data protection law aims to protect the fundamental right to data protection by giving data subjects control over their personal data and by setting limits on the collection and use of personal data. In the EU legal order, the right to data protection is recognised as a fundamental right in the Charter of Fundamental Rights of the European Union. Article 8(2) of the Charter stipulates that personal data must be

[37] Directive 98/6/EC of the European Parliament and of the Council of 16 February 1998 on consumer protection in the indication of the prices of products offered to consumers (Price Indication Directive) [1998] OJ L 80/27.

[38] Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising (Misleading and Comparative Advertising Directive) [2006] OJ L 376/21.

[39] Article 5 of the the Misleading and Comparative Advertising Directive.

[40] Article 4 of the the Misleading and Comparative Advertising Directive.

[41] Directive 98/27/EC of the European Parliament and of the Council of 19 May 1998 on injunctions for the protection of consumers' interests (Injunctions Directive) [1998] OJ L 166/51.

[42] See https://ec.europa.eu/info/law/law-topic/consumers/review-eu-consumer-law-new-deal-consumers_en.

processed fairly, for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. In addition, the right to data protection is enshrined in Article 16 TFEU, which was introduced in the Lisbon Treaty as the new legal basis for the adoption of secondary data protection legislation. The General Data Protection Regulation (GDPR),[43] which was adopted in April 2016 and which replaced the Data Protection Directive,[44] is based on Article 16 TFEU. Lastly, it is worth noting that in the context of the Council of Europe the right to privacy as contained in Article 8 of the European Convention on Human Rights has been interpreted by the European Court of Human Rights in Strasbourg to include a right to data protection as well.[45]

EU data protection legislation has thus recently transitioned from the Data Protection Directive, which was adopted in 1995, to the GDPR, which started to apply as of 25 May 2018.[46] These legislative instruments impose a number of obligations on controllers[47] and provide data subjects[48] with certain rights.

Article 5(1) of the GDPR contains the so-called data quality requirements, with which controllers have to comply and which form the main concepts of EU data protection law. These requirements consist of the notion of lawful, fair and transparent processing of personal data; purpose limitation; data minimisation; accuracy; storage limitation; and, as added in the GDPR, integrity and confidentiality. Lawfulness of processing requires the controller to have a legitimate ground to process personal data, such as consent of the data subject, performance of a contract, legal obligation or legitimate interests of the controller (see the legitimate grounds listed in Article 6(1) of the GDPR). The principle of purpose limitation entails that personal data has to be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Data minimisation calls for personal data to be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. In line with the requirement of accuracy, personal data has to be accurate and, where necessary, kept

[43] Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

[44] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) [1995] OJ L 281/31.

[45] See for example ECHR 16 February 2000, Amann v. Switzerland, No. 27798/95, ECLI:CE:ECHR:2000:0216JUD002779895, para. 65 and ECHR 4 May 2000, Rotaru v. Romania, No. 28341/95, ECLI:CE:ECHR:2000:0504JUD002834195, para. 43.

[46] Article 99(2) of the GDPR.

[47] The term 'controller' is defined under Article 4(7) of the GDPR 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*'.

[48] Article 4(1) of the GDPR defines a 'data subject' as '*an identified or identifiable natural person*' and specifies that '*an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*'.

up to date. The notion of storage limitation entails that personal data has to be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Finally, in accordance with the requirement of integrity and confidentiality, personal data has to be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

EU data protection law also provides data subjects with a number of rights. An illustrative example is the right of access contained in Article 15 of the GDPR, which entitles data subjects to obtain from the controller confirmation as to whether or not personal data are being processed, and, where that is the case, access to this data. It is important to note that the GDPR has introduced two new rights for data subjects: a right to erasure and a right to data portability.

As Article 17 of the GDPR makes clear, the right to erasure entitles data subjects to obtain from the controller the deletion of personal data in a number of situations, such as where the personal data are no longer necessary in relation to the purposes for which they were processed, where the data subject withdraws consent and no other legal ground for the processing remains, or where the data subject objects to the processing.[49] In *Google Spain*, the Court of Justice has already established a 'right to be delisted' with regard to the processing of personal data in the context of search engines. In its 2014 judgment, the Court held that a search-engine provider is responsible for the processing that it carries out of personal information which appears on web pages published by third parties. If, following a search made on the basis of a person's name, the list of results displays a link to a web page which contains information on the person in question, that person may approach the search-engine provider directly and request, under certain conditions, the removal of that link from the list of results.[50]

The right to data portability is provided by Article 20 of the GDPR and gives a data subject the right to receive his or her personal data that he or she has provided to a controller in a structured, commonly used and machine-readable format and to transmit this data to another controller.[51] Where technically feasible, the data subject also has the right to have the data transmitted directly from one controller to another.[52] In the latter situation, the data subject does not have to export and import the data him- or herself but can rely on the controllers, who must arrange the transfer of the data among themselves. The most commonly referred-to example of a service to which the right to data portability would apply is the social-network environment. In its Staff Working Paper accompanying the initial proposal for a General Data Protection Regulation, the Commission describes the personal data that may be transferred under the right to data portability as '*photos or a list of friends*' and

[49] Article 17(1) of the GDPR.

[50] ECJ, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, C-131/12, ECLI:EU:C:2014:317.

[51] Article 20(1) of the GDPR.

[52] Article 20(2) of the GDPR.

'*contact information, calendar history, interpersonal communications exchanges and other kinds of personally or socially relevant data*'.[53] The right to data portability thus enables users of social networks to transfer their profile, contacts, photos and videos to another social-networking platform. A Facebook user is, for instance, entitled to receive her personal data which she has provided to Facebook in a reusable format and to transmit this data to Google+. If technically feasible, she also has the right to have this data transmitted directly to Google+, instead of receiving the data from Facebook and transmitting it herself to Google+.[54]

2.4 Findings

Competition, consumer protection and data protection law advance various aspects of consumer welfare. EU competition enforcement aims to protect consumer welfare against the background of an economic and effects-based analysis, while EU data protection and consumer protection law follow a more human rights-based approach. Even though EU consumer protection law was initially established as a market-oriented policy, consumer protection is increasingly being conceptualised as a human right.[55] Its inclusion in the Charter of Fundamental Rights of the European Union may be the most apparent illustration of this development.

The means by which each of the three legal fields contributes to consumer welfare differ. Whereas the fields of consumer protection and data protection law seek to contribute to the functioning of the internal market through positive integration by adopting legislative instruments to harmonise national legislation in the Member States, competition policy is based on negative integration by ensuring that undertakings do not inhibit effective competition to the detriment of consumer welfare.[56]

As such, the three areas of law complement each other. While competition law advances consumer welfare by protecting undistorted competition, a precondition for the existence of a well-functioning market is that individuals are able to exercise a genuine and well-informed choice. To that end, the effective application and enforcement of information requirements in consumer protection law and conditions for valid consent in data protection law is instrumental. A minimum level of consumer and data protection is desirable to address possible externalities and persistent behavioural biases. Externalities are a form of market failure whereby an individual does not take into account the positive or negative impact of his or her

[53] Commission Staff Working Paper — Impact Assessment accompanying the General Data Protection Regulation and the Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (Impact Assessment Report), SEC(2012) 72 final, p. 28.

[54] Such a form of data portability would resemble number portability in the telecommunications sector. For a comparison, see Graef (2015b), 505-508.

[55] For a description of this evolution, see Benöhr (2013), 45-68.

[56] For a comparison of competition and data protection law in this respect, see Costa-Cabral / Lynskey (2017), 21-22.

behaviour on other individuals. In the data protection context, a disclosure of personal data by one individual may also affect others in case of shared preferences within a group of family or friends and even society at large when data is used to improve existing services or to develop new ones.[57] In addition, due to behavioural biases consumers do not always act rationally and may make decisions that are not in their own long-term interest.[58] While competition law aims to ensure the availability of choice, data protection and consumer protection law should empower individuals to effectively exercise such a choice. In conclusion, competition, data protection and consumer law have to go hand in hand in order to adequately protect the interests of individuals and consumer welfare in general.

In the following sections, the complementary nature of the three fields is illustrated by reference to three issues: the enforcement of data portability, the assessment of exploitative abuse under Article 102 TFEU and the potential role of data protection and consumer considerations in merger review.

3 Enforcement of Data Portability

As discussed above, the GDPR has introduced a right to data portability in EU data protection law. At the same time, competition and consumer protection law may be used to enforce data portability.

3.1 Competition Law Angle of Data Portability

Article 20 of the GDPR gives a data subject the right to receive personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and to transmit this data to another controller without hindrance from the controller to which the personal data has been provided. This right applies where the processing is carried out by automated means and is based on consent or on a contract.[59] Where technically feasible, the data subject also has the right to have the personal data transmitted directly from one controller to another.[60] While its main policy objective is to ensure that individuals are in control of their personal data and trust the online environment,[61] the right to data portability may also reduce lock-in by enabling users to switch easily between

[57] Larouche / Peitz / Purtova (2016), 30-31.

[58] See among others Acquisti / Brandimarte / Loewenstein (2015) and Acquisti / Taylor / Wagman (2016).

[59] Article 20(1) of the GDPR.

[60] Article 20(2) of the GDPR.

[61] Impact Assessment Report, p. 43.

services.[62] With the increasing use of a particular online service, the amount of personal data collected in this service may become an obstacle for moving to another provider, even if better or more privacy-friendly alternatives are available. As the Commission made clear in its Staff Working Document accompanying the proposal for a General Data Protection Regulation, the loss of data '*effectively creates a lock-in with the specific service for the user and makes it effectively very costly or even impossible to change provider and benefit from better services available on the market*'.[63] In this regard, data portability also has a competition law angle.

In fact, the previous Competition Commissioner argued in a speech that the proposed right to data portability '*goes to the heart of competition policy*' and that '*portability of data is important for those markets where effective competition requires that customers can switch by taking their own data with them*'. From a more general perspective, he stated that retention of data should not serve as a barrier to switching in markets that build on users uploading their personal data. In addition, the previous Competition Commissioner argued that '*[c]ustomers should not be locked in to a particular company just because they once trusted them with their content*'. By stating '*[w]hether this is a matter for regulation or competition policy, only time will tell*', he acknowledged the right to data portability as a new tool under data protection law but at the same time did not eliminate competition law intervention for facilitating data portability. In particular, the previous Competition Commissioner explicitly noted that '*[i]n time, personal data may well become a competition issue; for instance, if customers were prevented from switching from a company to another because they cannot carry their data along*'.[64]

It therefore cannot be ruled out that the European Commission will also intervene on the basis of competition law if a dominant firm does not allow users to take their data with them when switching services.[65] The *Facebook/WhatsApp* merger decision in which the Commission assessed whether data-portability issues constituted a barrier to consumers' switching in the context of consumer communications apps is instructive in this respect. The Commission made clear that it had not found any evidence suggesting that this was indeed the case. According to the Commission, 'communication via apps tends to consist to a significant extent of short, spontaneous chats, which do not necessarily carry long-term value for consumers'. The Commission also considered that the messaging history remains accessible on a user's smartphone even if the user starts using a different communications app. Finally, the Commission took into account that the contact list can be easily ported since a competing app, after obtaining consent of the user, would get access to his or her phone book, on the basis of which existing contacts can be

[62] For further guidance on how to apply the new right, see Article 29 Working Party (2017), which gives an interpretation of the conditions under which the right to data portability is applicable as well as its possible implementation.

[63] Impact Assessment Report, p. 28.

[64] Almunia (2012).

[65] Meyer (2012). See also Geradin / Kuschewsky (2013), 11.

identified.[66] Even though the Commission did not consider restrictions on data portability to constitute barriers to switching in the specific circumstances of the case, the fact that these issues were investigated under merger review indicates the potential of competition law to address data portability.

In particular, a refusal of a dominant firm to facilitate data portability may constitute a form of abuse by exploiting consumers or excluding competitors. In the latter case, a lack of data portability may lead to entry barriers for competitors and violate Article 102(b) TFEU by limiting markets and technical development to the prejudice of consumers.[67] In such a situation, the Commission can impose a duty on the dominant provider to give users the possibility to transfer their data to a competitor.

This can be further illustrated by the *Google* case, in which the Commission negotiated with Google about commitments which would force the search-engine provider to stop imposing obligations on advertisers that prevented them from moving their advertising campaigns to competing platforms.[68] In the US, the Federal Trade Commission closed its investigation when Google offered voluntary concessions to remove restrictions on AdWords that make it difficult for advertisers to manage advertising campaigns across multiple platforms.[69] By restricting the possibility of advertisers to move their campaigns to another advertising platform, providers create switching costs that may make advertisers decide to stay with their current provider for the sole reason that they find it too cumbersome to manually re-insert their advertising campaign in a new platform.

3.2 Comparing Data Protection and Competition Law

A number of differences can be identified between the enforcement of data portability under data protection law and competition law. First of all, it is important to note that the GDPR gives data subjects a right to data portability, while competition authorities can impose a duty on dominant providers to enable data portability if their behaviour amounts to abuse under Article 102 TFEU. Secondly, the scope of application of the two regimes is different. As it forms part of a data protection instrument, the right to data portability naturally only applies to transfers of personal data. Information that does not qualify as personal data falls outside the scope of the new right. In addition, one should note that not all personal data of a data subject is subject to the right to data portability. As Article 20(1) of the GDPR makes clear, a data subject is only entitled to

[66] European Commission, Case No. COMP/M.7217 – *Facebook/WhatsApp*, 3 October 2014, para. 113-115 and 134.

[67] Yoo (2012), 1154-1155 and Geradin / Kuschewsky (2013), 11.

[68] Commitments of Google in Case COMP/C-3/39.740 *Foundem and others*, 3 April 2013, para. 27-31.

In October 2013, Google offered improved commitments to the Commission that included a new proposal providing stronger guarantees against circumvention of the earlier commitments regarding portability of advertising campaigns; see Almunia (2013).

[69] US Federal Trade Commission, Press release: Google Agrees to Change Its Business Practices to Resolve FTC Competition Concerns In the Markets for Devices Like Smart Phones, Games and Tablets, and in Online Search, 3 January 2013.

port personal data which he or she has provided to a controller. But providers do not only possess personal data that has been provided by users themselves. They also obtain information about the behaviour of users on their platform (observed data) and create data for analytical purposes (inferred data). In accordance with the Article 29 Working Party Guidelines on data portability, inferred data falls outside the scope of the right to data portability. However, the Article 29 Working Party put forward the view that the term "provided data" has to be interpreted broadly not only covering 'data actively and knowingly provided by the data subject' but also 'observed data provided by the data subject by virtue of the use of the service or the device'. Despite the guidance offered by the Article 29 Working Party, uncertainties remain about the scope of the right to data portability. As an illustration, reference can be made to the profile of sellers on e-commerce platforms.[70] Whereas the contact information and the advertisements are provided by the seller him- or herself, the provider adds feedback scores to the seller's profile on the basis of the number of positive or negative ratings the seller has received. It is not clear whether the part of the seller's profile that involves the reputation that a seller has built on a particular e-commerce platform will also be portable under the right to data portability, since strictly interpreted it is not provided by the data subject nor observed by virtue of his or her use of a service.[71]

These limitations do not play a role in competition enforcement, where action can potentially be taken against a lack of portability of all data irrespective of whether it relates to an identified or identifiable natural person and whether it is provided by this person. The scope of application of competition law in this regard is thus much wider. At the same time, it has to be kept in mind that action on the basis of Article 102 TFEU can only be taken if the restrictions on data portability qualify as abuse of dominance. In contrast, the right to data portability would apply generally to all forms of processing carried out by automated means and based on consent or on a contract.[72] No dominance or abuse will have to be established in order for users to be able to transfer their data under the GDPR.[73] As such, data protection and competition law complement each other in enabling data portability. Each of the two fields has its own strengths and limitations, as a result of which it will remain important to apply competition law in parallel to possible restrictions on the portability of data once the right to data portability under the GDPR comes into force.

3.3 Possible Role of Consumer Protection Law

In addition, consumer protection law has a role to play in the enforcement of data portability. In this regard, it is instructive to note that the proposal for a Digital Content Directive includes a provision enabling a form of data portability. Article 13(2)(c) of

[70] Reference is made here to natural persons who are acting as sellers on e-commerce platforms, as the GDPR would otherwise not be applicable.

[71] See also Swire / Lagos (2013), 347-349.

[72] These are the preconditions for the right to data portability to apply under Article 20(1)(a) and (b) of the GDPR.

[73] Graef / Verschakelen / Valcke (2013), 7-8.

the proposal requires a supplier to provide a consumer who terminates a contract for the supply of digital content '*with technical means to retrieve all content provided by the consumer and any other data produced or generated through the consumer's use of the digital content to the extent that data has been retained by the supplier*'. The provision goes on to state that the consumer is '*entitled to retrieve the content free of charge, without significant inconvenience, in reasonable time and in a commonly used data format*'.[74] Article 3(1) of the proposal makes clear that the Digital Content Directive would apply to any contract where digital content, such as music or digital games, is supplied to a consumer and, in exchange, '*a price is to be paid or the consumer actively provides counter-performance other than money in the form of personal data or any other data*'.[75] For the purposes of the proposal for a Digital Content Directive, '*a service allowing sharing of and any other interaction with data in digital form provided by other users of the service*' is also regarded as 'digital content'.[76] Considering that a social network or a communications app thus falls within its scope of application, the Digital Content Directive would provide additional protection to consumers going beyond the right to data portability as contained in the GDPR.

Unlike the latter right, which only covers personal data provided by the data subject, Article 13(2)(c) of the proposal for a Digital Content Directive also enables a consumer to retrieve any other data, to the extent that it has been retained by the supplier, generated by using the digital content and not as such provided by the consumer. However, in the General Approach adopted by the Council in June 2017, the scope of the data to which the retrieval obligations would apply is limited to 'any digital content (…) to the extent that it does not constitute personal data, which was uploaded or created by the consumer when using the digital content or digital service supplied by the supplier'. This new formulation put forward by the Council seems to imply that inferred data would not be included. It therefore remains to be seen how the legislative discussions evolve and what the final scope of the data retrieval obligations will be.

On the other hand, it should be kept in mind that the proposal for a Digital Content Directive does not entitle consumers to have their digital content directly transmitted to a new provider. Article 20 of the GDPR, in contrast, provides data subjects with a right to ask for a direct transfer of provided personal data where this is technically feasible. These differences in scope can be explained by the distinct underlying objectives of the two instruments. While the right to data portability aims to give data subjects more control over their personal data, the relevant provision in the proposal for a Digital Content Directive aims to ensure that consumers benefit from effective protection in relation to the right to terminate the contract.[77]

Nevertheless, consumer protection law may fill the gaps that data protection and competition law currently leave with regard to the enforcement of data portability.

---

[74] Article 16(4)(b) of the proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content (proposal for a Digital Content Directive), 9 December 2015, COM(2015) 634 final, provides for a similar obligation for suppliers with regard to long term contracts for the supply of digital content.

[75] Article 3(1) of the proposal for a Digital Content Directive.

[76] Article 2(1)(c) of the proposal for a Digital Content Directive.

[77] Recital 39 of the proposal for a Digital Content Directive.

Consumer protection does not suffer from the inherent limitation of data protection law, which can only cover personal data and, unlike competition enforcement, it can enable data portability on a general basis for all providers irrespective of the existence of dominance and abusive behaviour. As such, consumer protection law may arguably form the most promising way to effectively enforce data portability. While the proposal for a Digital Content Directive already provides for the ability of users to retrieve the content provided and the data generated when leaving a service, a stronger and true form of data portability may be devised under consumer protection law which would enable users to directly transfer their data among services with the aim of empowering consumers to switch services.

4 Assessing Exploitative Abuse Under Article 102 TFEU

Even though competition law can be considered to have the strongest enforcement mechanism of the three fields in terms of the resources of the competent authorities and the available sanctions for infringements, it also has some weaknesses. One of them relates to assessing particular forms of abuse under Article 102 TFEU.

4.1 Excessive Pricing

A firm can abuse its dominant position in a particular market either by excluding competitors or by exploiting suppliers or customers. Although exclusionary and exploitative abusive behaviour can have an equally anticompetitive character, competition authorities rarely challenge behaviour that directly harms consumers and instead focus on addressing conduct of dominant firms leading to the foreclosure of competitors. It is also instructive to note in this respect that the European Commission has not provided any guidance relating to abusive exploitative conduct, while its Guidance Paper on exclusionary conduct under Article 102 TFEU was published in 2009.[78]

This may be explained by the fact that it remains complicated to establish at what point a certain type of exploitative behaviour becomes anticompetitive. These issues also play a role with regard to the assessment of possible abuses of dominance relating to the collection and use of data. A potential form of exploitative abuse that has been identified in this regard is the excessive extraction of personal information from users.[79]

Since personal data replaces price as a type of currency in the online environment, exploitative abuse may relate to the excessive collection of information about consumers instead of to the monetary price charged for a product or service. As Competition Commissioner Vestager made clear in a speech, the fact that consumers

[78] Guidance Paper, para. 28.

[79] See Autorité de la concurrence and Bundeskartellamt (2016), 25; UK House of Lords Select Committee on European Union (2016), para. 180; Monopolkommission (2015), para. 326 and 329 and Burnside (2015), 6.

pay with their data does not have to be a problem '*as long as people are happy that the data they share is a fair price to pay for the services they get in return*'.[80] The question thus arises what constitutes a 'fair price' in the context of data collection by dominant firms that provide services free of charge to consumers.

As regards excessive pricing, the Court of Justice argued in *United Brands* that '*a price which is excessive because it has no reasonable relation to the economic value of the product supplied*' is abusive under Article 102 TFEU.[81] In its Preliminary Opinion on 'Privacy and competitiveness in the age of big data', the European Data Protection Supervisor seems to rely on this statement of the Court of Justice in *United Brands* when noting that exploitative abuse may occur if '*the "price" paid through the surrender of personal information [is] to be considered excessive in relation to the value of the service consumed*'.[82] However, it will be complex to determine at what point the extent of data extraction is no longer in line with the value of the service.

Even though surveys and experiments may be held to determine the willingness of consumers to reveal certain information in exchange for being provided with a particular service,[83] it will be hard to prove a form of exploitative abuse relating to the extraction of personal data. As explained by the Monopolkommission, an independent expert committee that advises the German government and legislature in the area of competition policy, the services provided in the online environment may be so complex or user-specific that they require a situation- or user-dependent evaluation of the value of the service in question.[84] In addition, the heterogeneous preferences of consumers towards data protection may call for a user-specific analysis. While some consumers will not regard a particular form of data collection as excessive because they value the higher level of relevance and personalisation that it brings about, this may be different for consumers who are more sensitive to data protection issues. The excessive nature of prices is already difficult to determine under current competition law standards, let alone the excessive nature of the collection of personal data by a particular firm. To address this problem, relevant standards established in data protection and consumer law may help competition authorities to determine whether a certain form of data collection is anticompetitive under Article 102 TFEU.

4.2 Benchmarks from Data and Consumer Protection Law

Against this background, it has been proposed to rely on data protection principles as a benchmark against which the existence of abusive behaviour can be tested.[85] The head of the European Data Protection Supervisor Buttarelli stated in a 2015 speech that '*[w]e should be prepared for potential abuse of dominance cases which*

[80] Vestager (2016).

[81] ECJ, United Brands v. Commission, C-27/76, ECLI:EU:C:1978:22, para. 250.

[82] European Data Protection Supervisor (2014), 29.

[83] See OECD (2013), p. 29-32.

[84] Monopolkommission (2015), para. 329.

[85] See also Costa-Cabral / Lynskey (2017), 33-37.

also may involve a breach of data protection rules'.[86] In 2012, the then-Commissioner for Competition Almunia already referred to the possibility that '*[a] single dominant company could of course think to infringe privacy laws to gain an advantage over its competitors*'.[87] By collecting personal data beyond the consent of data subjects, a company can gain more insight into the preferences of individuals.

The investigation opened by the Bundeskartellamt in March 2016 on suspicion of Facebook's abuse of its possible dominant position in the market for social networks seems to be based on similar considerations. In particular, the Bundeskartellamt suspects that Facebook's terms of service are in violation of data protection law and thereby also represent an abusive imposition of unfair conditions on users. If a connection can be identified between the alleged data protection infringement and Facebook's possible dominance, the use of unlawful terms and conditions by Facebook could, in the view of the Bundeskartellamt, also be regarded as an abuse of dominance under competition law. In December 2017, the Bundeskartellamt reached the preliminary assessment that Facebook's collection and use of data from third-party sources is abusive. According to the Bundeskartellamt, Facebook is abusing its dominant position by making the use of its social network conditional on it being allowed to collect every kind of data generated by using third-party websites and merge it with the user's Facebook account. Considering that users are only given the choice of either accepting the "whole package" or not being able to use Facebook, the Bundeskartellamt takes the view that it cannot be assumed that users effectively consent to this form of data collection and processing.[88] The Bundeskartellamt thus appears to rely on data protection law as a benchmark for assessing whether certain exploitative behaviour of a dominant firm should be considered anticompetitive under Article 102 TFEU.

The investigation seems to relate to the question of whether consumers are sufficiently informed about the type and extent of personal data collected. The specific benchmark relied upon by the Bundeskartellamt to establish anticompetitive exploitation of consumers under abuse of dominance would then be the validity of consent under data protection law. In particular, the main focus of the investigation seems to be whether the consent given by Facebook users is sufficiently informed as required by Article 4(11) of the GDPR.

Alternatively, competition authorities may apply the purpose-limitation principle contained in Article 5(1)(b) of the GDPR or the principle of data minimisation derived from Article 5(1)(c) of the GDPR as benchmarks to establish abuse under Article 102 TFEU. Under these principles, controllers have to limit the collection of personal data to what is necessary to accomplish a specified and legitimate purpose and cannot retain data any longer than necessary to fulfil that purpose. In other words, if a firm extracts personal data beyond what is necessary to achieve a particular purpose or keeps it for a period longer than necessary to fulfil this purpose, it is violating

[86] Buttarelli (2015a), 3.

[87] Almunia (2012).

[88] Bundeskartellamt, Press release: Bundeskartellamt initiates proceeding against Facebook on suspicion of having abused its market power by infringing data protection rules, 2 March 2016 and Bundeskartellamt, Press release: Preliminary assessment in Facebook proceeding: Facebook's collection and use of data from third-party sources is abusive, 19 December 2017.

the data-minimisation and purpose-limitation principles. Such an infringement of data protection law may in turn also form an indication of whether the extraction of data is excessive and could qualify as exploitative abuse under competition law.

A similar analogy can be made with regard to principles used in consumer protection law. In speeches, the head of the European Data Protection Supervisor Buttarelli also referred to non-negotiable and misleading privacy policies as constituting a potential form of abuse of dominance.[89] It seems hard to determine at what point a (change in) privacy policy should give rise to competition law liability under Article 102 TFEU. Article 6(1) of the Unfair Commercial Practices Directive may be of assistance in this regard. According to this provision, a commercial practice has to '*be regarded as misleading if it contains false information and is therefore untruthful or in any way, including overall presentation, deceives or is likely to deceive the average consumer, even if the information is factually correct*' in relation to one or more of the elements specified in subsections (a) to (g) such as the nature of the product or its main characteristics. This is particularly relevant in Member States where the competition and consumer protection rules are enforced by the same authority. As an illustration, reference can be made to the two decisions that the Italian competition and consumer protection authority took in May 2017, imposing a fine of three million euros on WhatsApp for alleged unfair commercial practices. The first decision concluded that WhatsApp had forced users to subscribe to new terms and conditions by making them believe that otherwise they would not have been able to continue using the service. The second decision was directed at alleged unfair contract terms such as those relating to the right of WhatsApp to unilaterally change contractual provisions, the exclusive right of WhatsApp to terminate the service, exclusions and limitations of liability in favour of WhatsApp, the possibility of WhatsApp to interrupt the service without justifications and the choice of jurisdiction in case of disputes, which is currently exclusively assigned to US courts.[90] These decisions did not relate to potential breaches of competition law but of consumer protection law, for which the authority is also competent. However, the fact that the two regimes are enforced by one authority implies that the relevant expertise is present to rely on consumer protection principles in order to establish a violation of competition law in cases where this is desirable to enhance the effectiveness of the competition regime.[91]

By using principles from data protection or consumer protection law as benchmarks for analysing whether abuse of dominance under competition law exists, the difficulties that competition authorities currently face with regard to the assessment of exploitative abuse may be overcome. Such an approach could enable competition enforcement to address new forms of anticompetitive behaviour in digital markets. At the same time, caution is required to avoid outcomes whereby any law

[89] Buttarelli (2015b), 5 with respect to non-negotiable privacy policies; and Buttarelli (2015a), 3 as regards misleading privacy policies.

[90] Autorità garante della concorrenza e del mercato, Press release: WhatsApp fined for 3 million euro for having forced its users to share their personal data with Facebook, 12 May 2017.

[91] On the flip side, see Zingales (2017), 557-558, for a discussion of how the decisions of the Italian competition and consumer protection authority indicate the relevance of competition and data protection considerations in consumer law.

infringement by a dominant firm automatically becomes of relevance to competition enforcement. For that reason, commercial manipulation of personal data and privacy policies should remain an issue first and foremost tackled by data protection and consumer protection authorities. Nevertheless, if a strong link can be identified between a violation of data protection or consumer protection law and the dominant position of the infringer in the relevant market, there is no reason why a breach of one of these legal regimes cannot be a relevant factor for considering an independent violation of Article 102 TFEU.[92]

5 Potential Role of Data Protection and Consumer Law Considerations in Merger Review

The main weakness of data protection as well as consumer law as compared to competition enforcement is the limited scope for prospective analysis. In particular, the Directives of the EU consumer acquis as well as the GDPR do not give the respective supervisory authorities the competence to adopt structural measures to prevent possible future consumer or data protection issues from emerging. Consumer and data protection authorities can only impose behavioural remedies and sanction companies after the latter have infringed the rules by requiring changes in the way they deal with consumers or process personal data. Merger analysis under the competition rules, on the other hand, is forward-looking by nature and the EU Merger Regulation explicitly provides for the possibility to block mergers which are incompatible with the common market. On the basis of Articles 8(3) and 2(3) of the EU Merger Regulation, the Commission has to declare a proposed concentration as incompatible with the common market where it finds that the concentration would significantly impede effective competition as a result of the creation or strengthening of a dominant position. Because of the relative strength of merger review in this respect, the question arises whether consumer and data protection issues may be considered in the merger analysis to be conducted by competition authorities.

5.1 Current Reluctance of the Commission and the Court of Justice

Both the European Commission and the Court of Justice have already expressed views on the possible role of data protection concerns in EU competition law. The Commission did not take into account data protection interests when assessing the *Google/DoubleClick*, *Facebook/WhatsApp* and *Microsoft/LinkedIn* mergers. In the

[92] In the context of the abuse-of-dominance investigation against Facebook as announced by the Bundeskartellamt in March 2016, see Graef / Van Alsenoy (2016).

context of *Google/DoubleClick*, the Commission noted that its decision referred exclusively to the appraisal of the transaction with EU competition rules and was without prejudice to the obligations imposed on Google and DoubleClick by EU and national legislation in the field of data protection and privacy. In this regard, the Commission made clear that: '*Irrespective of the approval of the merger, the new entity is obliged in its day to day business to respect the fundamental rights recognised by all relevant instruments to its users, namely but not limited to privacy and data protection*'.[93] In its *Facebook/WhatsApp* merger decision, the Commission similarly stated: '*Any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules*'.[94] In the context of the *Microsoft/LinkedIn* merger, the Commission again argued in its press release that '*[p]rivacy-related concerns as such do not fall within the scope of EU competition law*' but continued by noting that such concerns '*can be taken into account in the competition assessment to the extent that consumers see it as a significant factor of quality, and the merging parties compete with each other on this factor*'.[95] Nevertheless, the issue at stake here goes beyond the possible inclusion of data protection as a factor of competition in the usual competition analysis and instead involves the question of whether competition enforcement can be used as a way to promote a stronger form of data protection.

While the Commission did not address data protection interests in these cases, it did analyse data-related competition concerns. In *Google/DoubleClick*, the Commission analysed the impact on the market of the potential combination of the previously separate datasets of the merging parties. The Commission argued that the combination of the information on search behaviour from Google and web-browsing behaviour from DoubleClick would not give the merged entity a competitive advantage that could not be matched by competitors, considering that such a combination of data was already available to a number of Google's competitors at the time of the proposed concentration. In the Commission's view, the possible combination of data after the merger would be very unlikely to bring more traffic to Google's AdSense network so as to squeeze out competitors and ultimately enable the merged entity to charge higher prices for its intermediation services.[96]

In *Facebook/WhatsApp*, the Commission analysed potential data-concentration issues in line with two theories of harm '*according to which Facebook could strengthen its position in online advertising*', namely by introducing advertising on

[93] European Commission, Case No. COMP/M.4731 – *Google/ DoubleClick*, 11 March 2008, para. 368.

[94] European Commission, Case No. COMP/M.7217 – *Facebook/WhatsApp*, 3 October 2014, para. 164.

[95] European Commission (2016), Press release (IP/16/4284) Mergers: Commission approves acquisition of LinkedIn by Microsoft, subject to conditions, 6 December 2016.

[96] European Commission, Case No. COMP/M.4731 – *Google/ DoubleClick*, 11 March 2008, para. 364-366.

WhatsApp and/or using WhatsApp as a potential source of user data for the purpose of improving the targeting of Facebook's advertising activities outside WhatsApp. The Commission concluded in this regard that the merger would not raise competition concerns, as there would continue to be a sufficient number of alternative providers to Facebook for the supply of targeted advertising after the merger, and a large amount of internet user data that is valuable for advertising purposes was not within Facebook's exclusive control.[97]

In *Microsoft/LinkedIn*, the Commission investigated several concerns relating to access to LinkedIn's database. In the area of professional social networks, the Commission expressed the concern that Microsoft would integrate LinkedIn into Microsoft Office and combine the two user databases. In particular, the Commission was worried that the increase in LinkedIn's user base would make it harder for new players to start providing professional social-network services and would tip the market towards LinkedIn in Member States where a competitor of LinkedIn operated, such as Austria, Germany and Poland. This could have been reinforced by shutting out LinkedIn's competitors from access to Microsoft's application programming interfaces which they need to access user data stored in the Microsoft cloud. The Commission found that these measures could have enabled LinkedIn to expand its user base and activity in a way that it would not have been able to do absent the merger.[98] To address this particular concern, Microsoft committed to grant competing professional social network service providers access to 'Microsoft Graph' for a period of 5 years. The latter is a gateway for software developers to build applications and services that can access data stored in the Microsoft cloud such as contact information, calendar information, emails etc. subject to user consent. The Commission expects that software developers may use this data to drive subscribers and usage to their professional social networks.[99] As to customer relationship management software solutions, the Commission looked at whether after the merger Microsoft would be able to shut out competitors by denying them access to the full LinkedIn database, thus preventing them from developing advanced customer relationship management functionalities. However, the Commission found that access to the full LinkedIn database was not essential to compete on the market.[100] With regard to online advertising, the Commission argued that no competition concerns arose from the concentration of the parties' user data that can be used for advertising purposes on the ground that a large amount of such user data would

[97] European Commission, Case No. COMP/M.7217 – *Facebook/WhatsApp*, 3 October 2014, para. 167-189.

[98] European Commission, Case No. M.8124 – *Microsoft/LinkedIn*, 6 December 2016, para. 337-351.

[99] European Commission, Case No. M.8124 – *Microsoft/LinkedIn*, 6 December 2016, para. 414 and 437. Additional commitments were adopted to address other identified competition concerns, namely concerns relating to the possible integration of LinkedIn features into Office and concerns relating to the possible pre-installation of a LinkedIn application on Windows PCs (see para. 409-421 and 434-438 of the decision).

[100] European Commission, Case No. M.8124 – *Microsoft/LinkedIn*, 6 December 2016, para. 274-276.

continue to be available on the market after the transaction. In addition, in the Commission's view, the transaction would not reduce the amount of data available to third parties, as neither Microsoft nor LinkedIn made its data available to third parties for advertising purposes at the time of the merger.[101]

Prior to these merger decisions, the Court of Justice had already made a statement in 2006 about the scope for data protection interests in EU competition policy in the context of a preliminary ruling involving agreements between financial institutions for the exchange of customer-solvency information. In its judgment in *Asnef-Equifax*, the Court noted that since '*any possible issues relating to the sensitivity of personal data are not, as such, a matter for competition law, they may be resolved on the basis of the relevant provisions governing data protection*'.[102] As a result, the Court seems to be of the view that data protection issues should, in principle, be addressed under data protection legislation rather than under the competition rules. In this respect, the Court's statement does not imply that data protection has no relevance to competition enforcement at all, but only seems to indicate that competition law should be applied in pursuit of the objectives underlying the discipline.[103] In essence, this is what the Commission did by leaving purely data protection-related interests aside and instead assessing possible competition concerns resulting from the combination of datasets or data concentration in *Google/DoubleClick*, *Facebook/WhatsApp* and *Microsoft/LinkedIn*.

5.2 Consumer and Data Protection as Legitimate Interests Under Merger Review

Since merger review is without prejudice to the obligations of the parties under data protection law, the approval of a transaction under the EU Merger Regulation does not prevent consumer or data protection authorities from initiating their own parallel investigation to examine whether the concentration raises any consumer or data protection issues. In order to achieve a better coordination between the European Commission as a competition authority and the national consumer and data protection authorities in this regard, Article 21(4) of the EU Merger Regulation may be relied upon by Member States. On the basis of this provision, Member States are entitled to take appropriate measures to protect legitimate interests other than those taken into account by the EU Merger Regulation. The *NewsCorp/BSkyB* merger can serve as an illustration in this regard. The Commission made clear in its merger decision that its analysis of the acquisition of BSkyB by NewsCorp was solely based on competition-related grounds under the EU Merger Regulation and was without prejudice to the

[101] European Commission, Case No. M.8124 – *Microsoft/LinkedIn*, 6 December 2016, para. 176-180.

[102] ECJ, Asnef-Equifax v. Asociación de Usuarios de Servicios Bancarios, C-238/05, ECLI:EU:C:2006:734, para. 63.

[103] Burnside (2015), 3-4.

media-plurality review of the relevant UK authorities.[104] While the Commission approved the merger on the basis of a competition assessment, Ofcom, the regulatory and competition authority for the broadcasting, communications and postal industries in the UK, required remedies from NewsCorp to address media-plurality issues.[105]

The legitimate interests that are specified in Article 21(4) of the EU Merger Regulation include public security, plurality of the media and prudential rules. Any other public interest must be communicated to the Commission by the Member State concerned, after which its compatibility with the general principles and other provisions of Community law will be assessed by the Commission. Consumer and data protection are not explicitly mentioned as legitimate interests, which means that a Member State has to notify the Commission of such potential public interests before it is entitled to take appropriate measures to this end on the national level.

It is important to note that the analysis conducted by a Member State under Article 21(4) takes place on the basis of national law and outside the framework of EU merger review. If a new public interest such as consumer or data protection should indeed be accepted by the Commission as a legitimate basis for adopting measures to protect non-efficiency considerations at the national level, the Member State may, on the basis of national law, subject a merger to additional conditions and may even block it if prohibiting the transaction altogether is proportionate in order to protect the public interest concerned. However, since EU consumer as well as data protection law do not provide the competent national authorities with the possibility to adopt any prospective or structural measures, it does not seem possible for a consumer or data protection authority to subject a merger to any conditions, let alone block it, if it does not give rise to consumer or data protection issues at the time the merger is approved by the Commission under the EU Merger Regulation.

A consumer or data protection authority would thus only be entitled to impose conditions to a merger under Article 21(4) of the EU Merger Regulation if the transaction in and of itself infringes consumer or data protection rules. If the supervisory authority merely anticipates that certain consumer or data protection issues might occur at some point in the future after the merger has been finalised, its only option is to monitor whether the merged entity continues to comply with its consumer or data protection obligations. Once there are indications that the merged entity is breaching the relevant rules, the authority may start an investigation on its own initiative on the basis of either consumer or data protection law and thus outside the framework of Article 21(4) of the EU Merger Regulation. The procedure under the latter provision therefore only seems to have relevance for mergers that at the time

[104] European Commission, Case No. COMP/M.5932 – *News Corp/ BSkyB*, 21 December 2010, para. 309.

[105] In June 2011, it was reported that NewsCorp had reached an agreement with Ofcom to clear the takeover on the condition that it would spin off BSkyB's dedicated news service Sky News into a separate company (see Sabbagh / Deans (2011)). However, in July 2011 NewsCorp withdrew its bid to take ownership of BSkyB following a scandal over phone hacking at NewsCorp's UK newspaper group (see 'News Corp withdraws bid for BSkyB', BBC News, 13 July 2011, available at: http://www.bbc.com/news/business-14142307).

of their notification to the Commission under EU merger review already raise either consumer or data protection issues.

Irrespective of the fact that the European Commission and the Court of Justice are currently hesitant towards the inclusion of data protection interests in competition law, the more normative question can be raised of whether the protection of this and other non-efficiency concerns like consumer protection should be considered in the competition analysis. The scope for such a more proactive approach is particularly apparent when conditions are imposed on a merger that raises economic-efficiency concerns. In this situation, the Commission as a competition authority could adopt conditions which not only address the economic-efficiency concerns but at the same time also guarantee the effectiveness of consumer and data protection law. In particular, the Commission could involve the competent national consumer or data protection authority in the implementation or even the monitoring of merger remedies that also affect consumer or data protection interests. In such a way, the current limitation of consumer and data protection law relating to the unavailability of prospective and structural measures may be addressed.

5.3 Illustrations of Data Protection-Related Merger Remedies

As an illustration of how merger remedies may be used to further data protection interests, reference can be made to the considerations involving the combination of datasets in *Google/DoubleClick*. Former US Federal Trade Commissioner Pamela Jones Harbour suggested in her dissenting statement that it may have been desirable to mandate a firewall between the data of Google and DoubleClick for some period of time to prevent any anticompetitive effects.[106] In such cases where the combination of datasets is considered to strengthen the position of the merged entity in a particular relevant market so as to significantly impede effective competition, the Commission could require the merging parties to keep their databases separate because of economic-efficiency concerns. It is instructive to note that the establishment of a firewall between the datasets of the merging parties would also prevent personal data from being used for incompatible purposes under EU data protection law. The Commission could then involve the competent data protection authority in the implementation of the merger remedies. This way, a remedy designed to address economic-efficiency concerns can be extended to include commitments with regard to how the merged entity will handle personal data after the merger. To ensure that the merged entity indeed keeps the datasets separate as committed to the Commission, the competent national data protection authority could be put in charge of monitoring to ensure that personal data is not exchanged between previously distinct services. This would also enable the data protection authority to require the merged

[106] Dissenting Statement of Commissioner Pamela Jones Harbour, *Google/DoubleClick*, FTC File No. 071-0170, 20 December 2007, footnote 23 on p. 9.

entity to take pre-emptive measures to prevent personal data from being combined and, as a consequence, used for incompatible purposes.

In hindsight, such a remedy might have been appropriate in *Facebook/WhatsApp* in light of the developments that have taken place since the Commission approved the merger in October 2014. Changes in WhatsApp's privacy policy were announced in August 2016 that enable Facebook to start using data from WhatsApp to better target ads on Facebook and Instagram.[107] This although Facebook's CEO Mark Zuckerberg at the time of the notification of the acquisition assured that no changes would take place in the way WhatsApp uses personal data from users.[108] The announcement of WhatsApp's new privacy policy has drawn concerns not only from national data protection and consumer authorities[109] but also from Competition Commissioner Vestager herself. Despite the fact that the Commission in its merger decision argued that the transaction did not raise competition concerns even if Facebook were to start collecting WhatsApp data to improve its own services,[110] the Commissioner followed up with Facebook to find out what was behind its decision to update WhatsApp's privacy policy.[111] This culminated in the imposition of a 110-million-euro fine by the Commission on Facebook in May 2017 for providing incorrect or misleading information during the 2014 merger investigation. While Facebook had informed the Commission that it would be unable to establish reliable automated matching between Facebook users' accounts and WhatsApp users' accounts, WhatsApp's updates to its terms of service in August 2016 included the possibility of linking WhatsApp users' phone numbers with Facebook users' identities. On that basis, the Commission found that the technical possibility of automatically matching Facebook and WhatsApp users' identities already existed in 2014 and that Facebook staff were aware of such a possibility. However, the fact that misleading information was given did not impact the 2014 authorisation of the transaction, as the decision was based on a number of elements going beyond automated user matching and the Commission at the time carried out the 'even if' assessment assuming user matching as a possibility.[112]

---

[107] WhatsApp blog, Looking ahead for WhatsApp, 25 August 2016, available at: https://blog.whatsapp.com/10000627/Looking-ahead-for-WhatsApp?l=en.

[108] Guynn (2014).

[109] Apart from the enforcement action of the Italian *Autorità garante della concorrenza e del mercato* mentioned in section 4.2 above, a number of authorities in other Member States have started investigations against Facebook. For an overview of these various national cases, see Zingales (2017), 554-555. In particular, the Article 29 Working Party is coordinating enforcement actions of national data protection authorities: see the Letter of the Chair of the Article 29 Working Party to WhatsApp, 27 October 2016.

[110] European Commission, Case No. COMP/M.7217 – *Facebook/WhatsApp*, 3 October 2014, para. 187-189.

[111] White / Levring (2016).

[112] European Commission, Press release (IP/17/1369), Mergers: Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover, 18 May 2017.

Nevertheless, one can raise the question of whether the Commission has not been too optimistic by approving the merger without even opening an in-depth investigation and exploring possible merger remedies.[113] Had the Commission taken a more proactive stance towards the data-concentration concerns in *Facebook/WhatsApp*, it could have prevented or at least restricted Facebook from unilaterally deciding to alter WhatsApp's privacy policy. The scope for merger remedies involving how personal data may be used after the merger was present, considering that the use by Facebook of data from WhatsApp also raised potential competition concerns. Now, in the absence of any merger remedies, the only option for the Commission and for the national data protection and consumer authorities is to monitor ex post whether Facebook is complying with the relevant rules. Considering that data protection and consumer rules are still enforced on a national basis, this leads to additional complexities in the sense that consumers may be subject to different levels of protection depending on the ability and success of the authorities in their respective territories to take action against Facebook.

6 Conclusion

Even though competition law, consumer and data protection law are different regimes having their own legal concepts and remedies, they share common goals. The three legal fields complement each other in protecting the general public and contributing to the achievement of the internal market. As such, three types of synergies have been identified where the different fields can help each other to reach the desired objective of protecting the welfare of individuals in digital markets.

With regard to the enforcement of data portability, data protection and competition law leave certain gaps due to the inherent limitations in their scope of application that may be filled by including a form of data portability in consumer protection law.

The assessment of exploitative abuse under Article 102 TFEU, in turn, may benefit from incorporating certain principles from data protection and consumer law as benchmarks on the basis of which competition authorities can determine at what point a form of data extraction or behaviour relating to the privacy policy of a dominant undertaking is to be considered as anticompetitive.

Finally, in the context of merger review, Article 21(4) of the EU Merger Regulation could be interpreted in such a way as to give consumer or data protection authorities a legal ground to review proposed concentrations on the basis of their impact on either consumer or data protection. Since EU consumer and data protection law do not provide for the possibility to adopt structural or prospective remedies, this provision does not make the agencies competent to block mergers on the

[113] The *Facebook/WhatsApp* merger was approved on the basis of Article 6(1)(b) of the EU Merger Regulation. See European Commission, Case No. COMP/M.7217 – *Facebook/WhatsApp*, 3 October 2014, para. 191.

basis of consumer or data protection considerations or to impose remedies to address possible future consumer or data protection issues. A more promising form of collaboration would be for the Commission to involve the competent consumer or data protection authority in the implementation or monitoring of merger remedies that also affect consumer or data protection interests. Apart from providing consumers with a more unified form of protection, this would also enable consumer and data protection authorities to engage in more proactive monitoring even if no violations of the relevant rules have yet been identified.

References

Acquisti, A. / Brandimarte, L. / Loewenstein, G. (2015), Privacy and human behavior in the age of information, 347 Science, 509-514

Acquisti, A. / Taylor, C. / Wagman, L. (2016), The Economics of Privacy, 54 Journal of Economic Literature, 442-492

Benöhr, I. (2013), EU Consumer Law and Human Rights, Oxford Studies in European Law

Burnside, A.J. (2015), No Such Thing as a Free Search: Antitrust and the Pursuit of Privacy Goals, 5 CPI Antitrust Chronicle, 1-8

Costa-Cabral, F. / Lynskey, O. (2017), Family Ties: The Intersection Between Data Protection and Competition in EU Law, 54 Common Market Law Review, 11-50

Cseres, K.J. (2007), The Controversies of the Consumer Welfare Standard, 3 Competition Law Review, 121-173

Geradin, D. / Kuschewsky, M. (2013), Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue, SSRN Working Paper February 2013, availabe at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2216088

Graef, I. (2015a), Market Definition and Market Power in Data: The Case of Online Platforms, 38 World Competition, 473-506

Graef, I. (2015b), Mandating portability and interoperability in online social networks: Regulatory and competition law issues in the European Union, 39 Telecommunications Policy, 502-514

Graef, I. (2016), EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility, Kluwer Law International

Graef, I. / Verschakelen, J. / Valcke, P. (2013), Putting the Right to Data Portability into a Competition Law Perspective, Law. The Journal of the Higher School of Economics. Annual Review, 53-63, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2416537

Kuner, C. / Cate, F.H. / Millard, C. / Svantesson, D.J.B. / Lynskey, O. (2014), When two worlds collide: the interface between competition law and data protection, 4 International Data Privacy Law, 247-248

Larouche, P. / Peitz, M. / Purtova, N. (2016), Consumer privacy in network industries, CERRE Policy Report 25 January 2016, available at: http://www.cerre.eu/sites/cerre/files/160125_CERRE_Privacy_Final.pdf

Nazzini, R. (2011), The Foundations of European Union Competition Law. The Objective and Principles of Article 102, Oxford University Press

Rousseva, E. / Marquis, M. (2013), Hell Freezes Over: A Climate Change for Assessing Exclusionary Conduct under Article 102 TFEU, 4 Journal of European Competition Law & Practice, 32-50

Swire, P. / Lagos, Y. (2013), Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique, 72 Maryland Law Review, 335-380

Van Rompuy, B. (2012), Economic Efficiency: The Sole Concern of Modern Antitrust Policy? Non-efficiency Considerations under Article 101 TFEU, Kluwer Law International

Yoo, C.S. (2012), When Antitrust Met Facebook, 19 George Mason Law Review, 1147-1162
Zimmer, D. (2012), The Goals of Competition Law, Edward Elgar
Zingales, N. (2017), Between a rock and two hard places: WhatsApp at the crossroad of competition, data protection and consumer law, 33 Computer Law & Security Review 2017, 553-558

Additional Sources

Almunia, J. (2012), Speech: Competition and personal data protection, Privacy Platform event: Competition and Privacy in Markets of Data Brussels, 26 November 2012, available at: http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm
Almunia, J. (2013), Speech: The Google antitrust case: what is at stake?, 1 October 2013, available at: http://europa.eu/rapid/press-release_SPEECH-13-768_en.htm
Article 29 Working Party, Guidelines on the right to data portability, 5 April 2017, 16/EN WP 242 rev.01
Article 29 Working Party, Letter of the Chair of the Article 29 Working Party to WhatsApp, 27 October 2016, available at: https://www.cnil.fr/sites/default/files/atoms/files/20161027_letter_of_the_chair_of_the_art_29_wp_whatsapp.pdf
Autorità garante della concorrenza e del mercato (2017), Press release: WhatsApp fined for 3 million euro for having forced its users to share their personal data with Facebook, 12 May 2017, available at: http://www.agcm.it/en/newsroom/press-releases/2380-whatsapp-fined-for-3-million-euro-for-having-forced-its-users-to-share-their-personal-data-with-facebook.html
Autorité de la concurrence and Bundeskartellamt (2016), Competition Law and Data, available at: http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf
Bundeskartellamt (2016), Press release: Bundeskartellamt initiates proceeding against Facebook on suspicion of having abused its market power by infringing data protection rules, 2 March 2016, available at: http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html?nn=3591568
Buttarelli, G. (2015a), Keynote speech at Joint ERA-EDPS seminar, workshop Competition Rebooted: Enforcement and personal data in digital markets Brussels, 24 September 2015, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2015/15-09-24_ERA_GB_EN.pdf
Buttarelli, G. (2015b), Speech: Privacy and Competition in the Digital Economy, Privacy Platform event: The Digital Economy, Competition and Privacy Brussels, 21 January 2015, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2015/15-01-21_speech_GB_EN.pdf
Commission Staff Working Paper — Impact Assessment accompanying the General Data Protection Regulation and the Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (Impact Assessment Report), SEC(2012) 72 final
Commitments of Google in Case COMP/C-3/39.740 *Foundem and others*, 3 April 2013, available at: http://ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_8608_5.pdf
Dissenting Statement of Commissioner Pamela Jones Harbour, *Google/DoubleClick*, FTC File No. 071-0170, 20 December 2007
European Commission (2016), Press release: Mergers: Commission approves acquisition of LinkedIn by Microsoft, subject to conditions, 6 December 2016, available at: http://europa.eu/rapid/press-release_IP-16-4284_en.htm
European Commission (2017), Press release: Mergers: Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover, 18 May 2017, available at: http://europa.eu/rapid/press-release_IP-17-1369_en.htm

European Data Protection Supervisor (2016), Opinion 8/2016 on coherent enforcement of fundamental rights in the age of big data, 23 September 2016, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Events/16-09-23_BigData_opinion_EN.pdf

European Data Protection Supervisor (2014), Preliminary Opinion. Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, March 2014, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf

Graef, I. / Van Alsenoy, B. (2016), Data protection Data protection through the lens of competition law: will Germany lead the way?, LSE Media Policy Project blog, 23 March 2016, available at: http://blogs.lse.ac.uk/mediapolicyproject/2016/03/23/data-protection-through-the-lens-of-competition-law-will-germany-lead-the-way/

Guynn, J. (2014), Privacy groups urge FTC to probe Facebook's deal to buy WhatsApp, *Los Angeles Times*, 6 March 2014, available at: http://www.latimes.com/business/technology/la-fi-tn-privacy-groups-urge-ftc-to-probe-facebooks-whatsapp-deal-20140306-story.html

Meyer, D. (2012), Facebook beware? EU antitrust chief warns over data portability, 27 November 2012, available at: http://www.zdnet.com/facebook-beware-eu-antitrust-chief-warns-over-data-portability-7000007950/

Monopolkommission (2015), Competition policy: The challenge of digital markets, Special report No. 68, July 2015, available at: http://www.monopolkommission.de/images/PDF/SG/s68_fulltext_eng.pdf

News Corp withdraws bid for BSkyB, BBC News, 13 July 2011, available at: http://www.bbc.com/news/business-14142307

OECD (2013), Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, *OECD Digital Economy Papers*, No. 220, 2013, 29-32, available at: https://doi.org/10.1787/5k486qtxldmq-en

Sabbagh, D. / Deans, J. (2011), News Corp's BSkyB bid: Jeremy Hunt expected to give green light next week, The Guardian, 23 June 2011, available at: http://www.theguardian.com/media/2011/jun/22/news-corp-bskyb-jeremy-hunt

UK House of Lords Select Committee on European Union (2016), Online Platforms and the Digital Single Market, 10th Report of Session 2015-16, 20 April 2016, available at: http://www.publications.parliament.uk/pa/ld201516/ldselect/ldeucom/129/129.pdf

US Federal Trade Commission (2013), Press release: Google Agrees to Change Its Business Practices to Resolve FTC Competition Concerns In the Markets for Devices Like Smart Phones, Games and Tablets, and in Online Search, 3 January 2013, available at: http://www.ftc.gov/news-events/press-releases/2013/01/google-agrees-change-its-business-practices-resolve-ftc

Vestager, M. (2016), Speech: Making data work for us, Data Ethics event on Data as Power Copenhagen, 9 September 2016, available at: https://ec.europa.eu/commission/2014-2019/vestager/announcements/making-data-work-us_en

WhatsApp blog, Looking ahead for WhatsApp, 25 August 2016, available at: https://blog.whatsapp.com/10000627/Looking-ahead-for-WhatsApp?l=en

White, A. / Levring, P. (2016), Facebook Grilled by EU's Vestager Over WhatsApp Merger U-Turn, 9 September 2016, available at: http://www.bloomberg.com/news/articles/2016-09-09/facebook-grilled-by-eu-s-vestager-over-whatsapp-merger-u-turn

The Rise of Big Data and the Loss of Privacy

Anca D. Chirita

Contents

1 Introduction 154
2 Why Big Data Matters 156
3 Privacy as a Fundamental Economic Right 159
4 Informed Consent 163
5 The Case for Competition Intervention Against Targeted Advertising 165
6 A Comparative Assessment of Case Studies of Privacy 172
6.1 A Classification of the 'Big Data' Collection 175
6.2 Data Sharing 180
6.3 Consent 181
6.4 Disclosure of Data 183
7 A Response from Practice: Vidal-Hall v Google Inc [2015] EWCA 183
8 Conclusions 185
References 185

Abstract This chapter offers a classification of personal data based on the study of privacy policies of Google, Microsoft Windows, Facebook, Instagram, Linked-In,

Anca D. Chirita, Lecturer in Competition Law (Dr. iur.), Durham University, UK. Earlier drafts of this article benefited from insightful suggestions and comments from the attendees of the 15th Conference of the International Association of Consumer Law organised by the Amsterdam Centre for the Study of European Contract Law on a presentation entitled 'Consumer Rights, Misleading Advertising and Privacy in the Digital Age' in June 2015; LLM students taking a research-led competition-law seminar at Durham University in March 2016; the Durham Law School Staff Seminar Series 2015/2016 in May 2016, with special thanks to Aoife O'Donoghue, Se-Shauna Wheatle, Annika Jones, Johanna Jacques, Andrés Delgado Casteleiro, Henry Jones and Professors Thom Brooks and John Linarelli; and the attendees of the conference on 'Personal Data in Competition, Consumer Protection and IP Law: Towards a Holistic Approach' at the Max Planck Institute for Innovation and Competition in Munich in October 2016, in particular to Beatriz Conde Gallego and Gintare Surblyte. The chapter is dedicated to my sister, Andra Chirita, an IT developer, in loving memory.

A. D. Chirita (✉)
Durham University, Durham, UK
e-mail: a.d.chirita@durham.ac.uk

M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law*, MPI Studies on Intellectual Property and Competition Law 28, https://doi.org/10.1007/978-3-662-57646-5_7

and Whisper. It argues that online price discrimination contributes to higher corporate profits and economic inequality. Competition policy intervention is therefore needed to curb this inequality that generates a false impression that a few digital giants are competing on the merit of their 'highly innovative' data-driven products and performance. The chapter argues that knowing a consumer's usage, frequency, preferences, and choices disempowers online consumers.

1 Introduction

This chapter explains why 'big' data matters and why privacy is now lost as a social norm. In its Opinion, the European Data Protection Supervisor suggested a consumer protection approach to data owned by monopolists.[1] It relied on the essential facility doctrine of intervention where a smaller entrant is foreclosed because it cannot access the data owned by the monopolist. The German competition authority subsequently indicated that access to data is a factor indicative of market power.[2]

Both the Opinion and the doctrine of essential facilities[3] are now of little help to competition authorities. Instead, this chapter will evaluate the legal framework to clarify the scope of application of the data protection rules and elucidate whether competition intervention in this context has any merit in its own right. Articles 7 and 8 of the EU Charter of Fundamental Rights and the former Directive 95/46/EC will be mentioned before the chapter fully engages with the recent developments in the area of data protection. In particular, drawing on the risks associated with data processing in both Directive EU/2016/680 and Regulation EU/2016/679, the chapter seeks to determine how price discrimination can actually happen in the form of abuse of personal data. The latter carries an economic significance, as through the misuse of such data, consumers can be left worse off when bargaining or shopping online. Further risks associated with the processing of personal data concern health, which could, in turn, raise life insurance premium rates. In other cases, personal data can reveal a particular economic situation, personal preferences or interests, reliability, or behaviour, which could make price discrimination much easier.

The new regulation mentions the risks associated with online activity and the need to overcome different rules on the protection of personal data, which could distort competition. The major provision is one which explains that the Regulation does not apply to a 'purely personal or household activity', including social networking and online activity. This is to be interpreted in the sense that data protection

[1] See European Data Protection Supervisor (2014).

[2] Bundeskartellamt, Press Release: Bundeskartellamt initiates proceeding against Facebook on suspicion of having abused its market power by infringing data protection rules, 2 March 2016, 16; for the view that data can be a source of market power, see Drexl / Hilty / Desaunettes / Greiner / Kim / Richter / Surblytė / Wiedemann (2016).

[3] For the view that the doctrine is potentially misleading, as rivals are not prevented from collecting data themselves, see Schepp / Wambach (2016), 123.

and supervision do not have as a purpose safeguarding the online privacy of individuals. This is significant since many influential commentators have long held that competition law should not become a regulatory tool for intervention in the area of personal data protection.[4] Nonetheless, the regulatory approach to data processing aims primarily to protect employees from businesses that process personal data and that could lawfully disclose such data to the competent authorities in the wake of various investigations. However, the present framework can easily be abused or misused. It is broad on potential data subjects, as it includes 'persons possessing relevant information or contacts'. So anyone's personal data could be saved for unknown purposes.

The chapter moves on to critically review the position of mere silence or inaction in the case of default settings of social networks or web browsers to review the position of informed consent under the new Regulation. The chapter argues that recent theories of informed consent place particular emphasis upon the degree of sophistication and the length of privacy policies, rather than affirmative box ticking. There is hidden 'small print' or pitfalls, such as 'improving customer experience', which make it possible to process personal data without a just cause.

The chapter examines Windows 10, Google, Facebook, Linked-In, Instagram, Snapchat, and Whisper's privacy policies to establish compliance with data protection and reveal which distinctive categories of personal data are being processed. Existing evidence of price discrimination will be used to extract the pitfalls associated with social platforms based on trust and the potential abuse of consumer confidence that such data is safe from being shared with third parties. Although there are warnings regarding the selling of data, this chapter will remain focused on the big data owned by the three main companies, namely, Google, Facebook, and Microsoft. The selling of personal data could potentially lead competition authorities to uncover the bid-rigging of markets for personal data, which could extend competition intervention to include more 'secretive' social media, such as Whisper, Snapchat, or Instagram. Installed software and browsers can also be used as a means to improve users' experience, but the processing of sensitive and confidential data has little to do with this purpose.

This author agrees with the merits of the dissenting opinions by the late Commissioner Rosch and Commissioner Jones Harbour, though this author argues that the EU Commission's intervention is warranted by the enactment of the new rules on data protection, in particular, by what these rules have now left outside their material scope. Relying on Stiglitz's theory of economic inequality, this chapter argues in favour of considering data as the new currency in two-sided markets. While Google's sale of its users' privacy to third parties has famously been described as 'Googlestroika', namely, a 'privacy derivative', this zero-priced product[5] remains problematic through the sharing of personal data with third parties.

[4] Recently, it has rightfully been argued that less intervention is inappropriate; see Kadar (2015).

[5] It is interesting to note that, according to a leading economist, 'Free is a number; it is the price of zero', see the Witness Evidence provided by Evans / Ezrachi (2015), 10; see e.g. Schepp / Wambach (2016), 123, who argued in favour of competition intervention based on data protection and privacy as 'elements of non-price competition'; see e.g. Martens (2016), 38, who argued that the widespread market failure of privacy-informed decisions by consumers could pave the way for regulatory intervention.

In conclusion, the chapter adds the abuse of personal data to the non-exhaustive list of abuse of dominance.[6] This abuse happens on online platforms, which are outside the scope of data-protection laws. Such platforms misuse the trust and confidence of individual users by making them reveal personal data and by encouraging users to voluntarily consent to the transfer of personal data to third parties. Personal preferences or choices are later shared with advertisers and sellers and used to engage in price discrimination. Indeed, online price discrimination and booking manipulation based on users' personal data is now a social norm. Ultimately, data-protection laws are useless in practice,[7] as they solely highlight the need to educate consumers and raise awareness. There is, therefore, one active remedy left: the intervention of competition policy.

2 Why Big Data Matters

All businesses, including public institutions, may possess and/or process some form of personal data. This chapter is not concerned about the mere possession of personal data by a dominant market player. Rather, it seeks to highlight how personal data, which is economically relevant, could be misused, for instance, through it being shared with third parties, in order to maintain or strengthen a dominant market position. Furthermore, this chapter also wishes to signal a potential bid-rigging of personal data by colluding undertakings, including popular social media, under Article 101 TFEU.

This chapter acknowledges that a potential misuse of personal data by dominant undertakings has no precedent line of case law. While its novelty could trigger this particular form of abuse to be affixed with an exotic label, as it sits outside the confines of traditional competition practice under Article 102 TFEU, it is never to be underestimated by dominant undertakings that actively engage in the sharing, transferring, or selling of such data.

The author is grateful to the Commissioner for Competition, Margrethe Vestager, for bringing data concerns to the competition policy's discourse. In her recent speech,[8] Commissioner Vestager said, 'a lot of people tell me they're worried about how companies are using their data. I take those worries very seriously. Privacy is a fundamental part of our autonomy as individuals. We must have the right to decide who we share our information with, and for what purpose.'

This is the first time that privacy considerations have formed part of meaningful competition policy rhetoric. And this rhetoric can also succeed when these considerations are properly identified and given an economic dimension, which this

[6] Again proving Hayek's assertion right, namely, that competition is a process of discovery, this time in the area of new information economics; see Hayek (2002), 9-23.

[7] For the view that data-protection law is unable to address the concerns of individuals regarding personal data processing by platforms, see London School of Economics (2015).

[8] Vestager (2016); Committee of Economic and Monetary Affairs (2014), 4-056.

chapter will seek to achieve in the next sections. It is not a new topic, however: in the 1980s, US scholars were preoccupied by privacy. While Posner's concept of privacy[9] appears limited for current purposes, it nonetheless represents a historical moment for privacy. Initially, Posner looked at potential labour market asymmetries if employers were not able to have personal data about their future employees. Disclosure was, therefore, seen as mandatory for employees with criminal records. This context of employment relations led Posner to consider privacy as being 'harmful to efficiency' where a lack of disclosure could prevent an efficient exchange of labour. Similarly, Hermalin and Katz argued that, due to these information asymmetries caused by non-disclosure, an individual with poor health could opportunistically take advantage of life insurance.[10] However, such cases are very limited.

For Stigler, privacy is a subject of public policy,[11] whose purpose is 'the possession and acquisition of knowledge about people'. In practice, privacy acts as a shield that restricts the collection or use of personal data about an individual or corporation.[12]

A notable academic commentator had previously remarked that 'the loss of individual privacy … is often framed more around an individual sense of unease at the surveillance of peoples' lives than how a shift in knowledge about individuals to corporate hands should force us to re-evaluate our economic models and regulatory tools'.[13]

This chapter raises no expectation that competition authorities will tackle the complex issues surrounding individuals' surveillance at large.[14] Instead, the chapter aims to elevate the normative value of privacy as an economic right that is not devalued by public competition enforcement as being solely a human right of the public, which has to be addressed elsewhere and through other means, e.g. consumer or data-protection law. Beyond any doubt, competition authorities will have to adapt their traditional law-and-economics analysis in order to be able to deal with a monopolistic abuse of personal data in digital markets for two main reasons.

First, it is uncontroversial to suggest that personal data owned by companies has, indeed, an economic value attached to it. In the words of the EU Commissioner, such data has become the 'new currency.'[15] Previously, the European Data Protection Supervisor recognised that while '[c]onsumers provide richly detailed information about their preferences through their online activities … personal information

[9] See Posner (1980), 405-409.

[10] See Hermalin / Katz (2006), 211.

[11] See Stigler (1980), 624.

[12] Ibid., 625.

[13] Newman (2014a), 852.

[14] See Joyce (2015), 3. This chapter leaves outside its scope the implications of the recently enacted UK Investigatory Powers Act, which received Royal Assent on 28 November 2016, available at: http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted/data.htm.

[15] Vestager (2016). Similarly, when providing his expert witness on online platforms, Professor Ezrachi suggested that 'the engine, the fire at the heart of this market, is definitely data'; see Evans / Ezrachi (2015), 15.

operates as a currency, and sometimes the sole currency, in the exchange for online services'.[16]

Therefore, it is uncontroversial to consider the owners of personal data as consumers of online products or services, from search engines or shopping to social or professional media. While trading and entertainment follow different purposes, both can intersect each other; this blurs the distinction between private and public spheres. An axiomatic reduction of competition policy's objectives to enhance consumer welfare[17] means that once a company sells a product for free, but the sum of its individual consumers pays nothing more in return than the naïve confidence that any personal preferences, economic interests or behaviour will be kept private, this is an exploitative abuse. Through invasive techniques of data sharing, such companies are guilty of misusing personal data for extracting an economic profit. Personal, private data becomes then public data owned by third parties so that dominant undertakings can further consolidate their dominant position. This has absolutely nothing to do with competition on the merit. If a product or service is promised for free, but the seller charges a bill for it later, then that product or service is called 'personal data': 'if just a few companies control the data you need to satisfy customers and cut costs, that could give them power to drive their rivals out of the market.[18]

Second, it would be controversial to identify an anti-competitive practice where a few undertakings controlled big data but used it to eliminate their smaller competitors.[19] Moving in this direction, a recent joint report by the French and German competition authorities has rightfully identified that data itself is 'non rivalrous',[20] while examining the existence of a sufficiently large customer base, network effects, and barriers to market entry.[21]

While the orthodoxy of exclusionary abuse dominates past competition practice, it is by no means a universal remedy for abuse in the present setting. As revealed by various commentators, exploitative abuse[22] often remains unchallenged and underenforced, as it asks competition authorities to put forward evidence of any anti-competitive harm. For competition and data enforcers, this can easily turn into a daunting task of hunting for hidden evidence of data misuse.

The European Data Protection Supervisor had a similar exclusionary vision in hindsight. It duly acknowledged that 'powerful or dominant undertakings are able

[16] European Data Protection Supervisor (2014), para. 2.2.10.

[17] For the argument that consumer law is now closer to the goals of EU competition law, see Albors-Llorens (2014), 173; on the potential to incorporate consumer-law requirements into competition policy, see Chirita (2010), 418.

[18] See n 16 above.

[19] See Pasquale (2013), 1009; for the contrary opinion, see Lerner (2014), 19.

[20] Lerner (2014), 21, for the same finding see e.g. Martens (2016), 38.

[21] Autorité de la concurrence and Bundeskartellamt (2016), thus the report relies on the old Directive.

[22] For the view that some anti-competitive practices may be both exclusionary and exploitative, see Bellamy / Child (2013), 10064; O'Donoghue / Padilla (2006), 194; for an explanation of the two concepts, see Whish / Bailey (2015), 212.

to exploit "economies of aggregation" and create barriers to entry through the control of huge personal datasets'.[23] However, as every dominant, or even non-dominant, company should take full responsibility for its datasets, barriers to entry are never the culprit of the real problem. Raising barriers to entry is costly for competitors, but, as digital products or services are offered for free in exchange for personal data, such dominant companies cannot produce them any more cheaply. Therefore, digging into a hole, i.e. the essential facility doctrine, and seeing dominant companies as gatekeepers of big data who exclude smaller rivals, is nothing but a false premise. The actual problem can be solved only by proving that the data in question is the price to be paid and that privacy can be translated into monetary terms. To put it another way, this chapter argues that competition intervention against 'big data' monopolists should be based on identifiable economic harm to consumers of digital products or services as a result of exploitation of their naïve trust and confidence. It should not be based solely on crude and rivalrous exclusionary abuse through harm inflicted on other competitors who are attempting to possess the same relevant data.

3 Privacy as a Fundamental Economic Right

Many articles have already been written on the provisions of the EU Charter of Fundamental Rights offering individual protection against interference by the state in the private sphere (Article 7) and beyond to protect personal data (Article 8).[24] This fundamental protection creates an expectation that privacy disclosures are an exception rather than the norm. In sharp contrast, Facebook's owner, Zuckerberg, has claimed that 'privacy is disappearing as a social norm'.[25] However, as the recent investigation of the German competition authority demonstrates, not even Facebook is immune to competition intervention.[26] Article 8's exceptional requirements, namely, the fairness and lawfulness of the data processing for a specified purpose, and transparency, including the right of access to data, are to be considered as setting the constitutional dimension of privacy.[27] The former Directive 95/46/EC[28]

[23] European Data Protection Supervisor (2014), para. 3.1.4.

[24] See Lynskey (2014a), 569-597; in the UK, data protection has been seen as a facet of privacy; see Lynskey (2015), 529; Roberts (2015), 544; Lynskey (2014b), 1800.

[25] See the Guardian, Privacy No Longer a Social Norm, Says Facebook Founder, 10 January 2010.

[26] Bundeskartellamt, Press Release: Bundeskartellamt initiates proceeding against Facebook on suspicion of having abused its market power by infringing data protection rules, 2 March 2016.

[27] See, for instance, the constitutional controversy raised by the German bill on data retention, which was criticised by the Federal Data Protection Commissioner as a disproportionate violation of Germans' basic civil rights: Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (2015), *Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten*, BT-Drucksache 18/5088.

[28] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to personal data and on the movement of such data, [1995] OJ L 281.

conferred individual protection of personal data. Article 2 referred to 'any information relating to an identified or identifiable natural person'. Following this line, privacy entails certain subjective attributes, such as the identity, characteristics, or behaviour of an individual. In particular, Article 6(1) of the Directive laid down some fundamental principles of data protection. These principles aim to ensure trust, predictability, legal certainty, and transparent use of personal data by data controllers. The collection of personal data is rather exceptional, namely, for 'specific, explicit and legitimate purposes'. Any data processing should be compatible with these purposes. The new EU Directive 2016/680 is more helpful in delimiting the above purposes, namely the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties.[29] Recital 26 in conjunction with Article 46(1) aims to raise awareness of the risks, rules, safeguards, and rights in relation to the processing of personal data. While 'awareness raising' resonates with the right of consumers to information and education, as embedded in Article 169 of the TFEU, the economic interests of consumers are simply put in jeopardy by this lax approach. Again, the European Data Protection Supervisor had previously warned: 'While many consumers may be becoming more and more 'tech savvy', most appear unaware of or unconcerned by the degree of intrusiveness into their searches and emails as information on their online activities is logged, analysed and converted into revenue by service providers.'[30]

The material scope of personal data processing remains guided by the principles of lawfulness, i.e. that it be necessary for the performance of a task carried out in the public interest by a competent authority[31]; adequacy and relevance, i.e. for the purpose for which data is processed[32]; transparency,[33] i.e. the right to know about the various purposes of data processing; and proportionality, i.e. data should not be kept longer than necessary unless data processing could be reasonably fulfilled by other means. In the forthcoming section detailing particular case studies, it will be demonstrated how, in practice, big companies collect an excess of personal data.

Under 'data subjects',[34] the Directive includes as addressees of data protection suspects, persons convicted of a criminal offence, victims, and other parties, such as witnesses, persons possessing relevant information or contacts, and associates of suspects and convicted criminals. Given that anyone could be within a circle or network of contacts, which could eventually reveal sensitive information, there is a great potential for the misuse or abuse of data processing.

---

[29] Directive EU/2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, [2016] OJ L 119/89.

[30] European Data Protection Supervisor (2014), para. 2.4.14.

[31] See Recital 35 of the new Directive.

[32] Ibid., Article 4 (1).

[33] Ibid., Recital 43.

[34] Ibid., Recital 31 in conjunction with Article 6.

Turning back to the previously alluded to risks associated with the rights and freedoms resulting from data processing, both the EU Directive 2016/680[35] and Regulation 2016/679[36] include a long list of potential personal damage due to, for example, discrimination, identity theft or fraud, financial loss, loss of confidentiality, unauthorised reversal of pseudonymisation, or other 'significant economic or social disadvantage'. Some of them have a strong link to competition practice, in particular where the data could be processed for engaging in price discrimination. The latter anti-competitive practice[37] could cause financial losses during shopping or bargaining due to the misuse of personal data about an economic or social condition. Again, this demonstrates that, by ignoring privacy considerations that carry an economic significance, competition authorities could miss out on many opportunities to uncover anti-competitive misuse and abuse of data. Of course, discrimination can be based on many other subjective factors, such as racial or ethnic origin, political opinions, religion, sexual orientation[38] and so on, and so these are not necessarily used for economic or price discrimination. In *Digital Rights Ireland*,[39] the ECJ considered that: 'To establish the existence of an interference with the fundamental right to privacy, it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way'.[40]

Other sensitive data, such as genetic, biometric, or health data, could lead to price discrimination against individuals in their daily life, for example, when applying for life insurance.[41] For those competition authorities that have, in recent years, adjusted their enforcement efforts to consider aspects of behavioural economics,[42] Regulation 2016/679 places 'personal preferences or interests, reliability or behaviour' in the spotlight of evaluating personal aspects of data subjects' lives. The processing of such behavioural data could also lead to price

[35] Ibid., Recital 51.

[36] See Recital 75 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1.

[37] Generally on price discrimination, see Bergemann / Brooks / Morris (2015), 921; Baker (2003), 646; Armstrong / Vickers (2001), 579; against regulating price discrimination, see Cooper (1977), 982.

[38] For example, Facebook's users could be targeted with specific advertising based on certain characteristics, such as 'interested in women or men', which have been entered in their profile, see Heffetz / Ligett (2014), 81.

[39] ECJ, Digital Rights Ireland and Seitlinger and others, C-293/12 and C-594/12, ECLI:EU:C:2014:238, para. 33.

[40] Ibid., para. 33.

[41] See Evans (2009), 50, who considers the possibility that advertisers could infer from an individual's online behaviour whether the user falls under a low or high insurance risk.

[42] For an excellent book on behavioural economics of consumer contracts, see Barr-Gill (2012), 7; on the limits of competition and the necessity of adding behavioural economics to include misperception and bias caused by asymmetric information available to consumers, 16.

discrimination. The same applies to aspects concerning economic situation, location, or movements. Ultimately, if personal details are known, those who possess them could engage in price wars based on someone's economic, social, physiological, or health, i.e. genetic or mental condition.[43]

So, how are these categories of personal data linked to competition? One of the most significant provisions of Regulation 2016/679 is Recital 2's reference to the accomplishment of an 'economic union', to 'economic and social progress', and to the 'well-being of natural persons'. While economic goals match competition policy's goals, consumer well-being is, indeed, wider than welfare. However, having regard to earlier considerations, online-privacy law[44] affects the well-being of individuals but could be translated into economics of privacy. In other words, personal data forms an integral part of the economic calculus. Contributing to closing the gap between privacy and competition is Roberts' recognition of a right to privacy, whose function is 'to prevent others from acquiring *dominating* power'.[45] In essence, this conceptual threshold advanced by public law matches perfectly that used by the same preventive function of abuse of dominant market power under competition laws.

Another significant provision is Recital 9 of the above Regulation, which acknowledges a 'widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity'. This becomes problematic because of existing differences in the level of data protection. It is yet another 'obstacle to the pursuit of economic activities' which could 'distort competition'.

The material scope of the application of Regulation 2016/679 is reinforced by Recital 18, which makes it clear that the Regulation does not apply to the 'processing of personal data in the course of a purely personal or household activity'. This may include 'correspondence, the holding of addresses, or social networking and online activity undertaken within the context of such activities'.[46] As long as online searching, browsing, or social media interactions have 'no connection to a professional or commercial activity', Regulation 2016/679 does not apply. This is of great significance for competition authorities. Many commentators have been dismissive of a potential competition law intervention in this area without offering any compelling reasons for non-intervention. Therefore, by making a clear distinction between the public and the professional profile of an employee and the private regime applicable to personal data, the Regulation leaves untouched a grey area of big data

[43] See Article 3(1) of the Regulation on personal data that could be used to identify someone after name, location, or online identifier and other subjective factors.

[44] See Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, known as the Directive on privacy and electronic communications, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, [2009] OJ L 337/11.

[45] Roberts (2015), 546 (emphasis added).

[46] See Recital 18 of the new Regulation.

owned by digital monopolists. The dangers of monitoring individual behaviour or internet tracking or of profiling for analysing or predicting an individual's own personal preferences, behaviour, and attitudes, could never have been made clearer than in Recital 24, albeit in a professional context.

To date, there is no economic regulation applicable to digital monopolies that process personal data unrelated to employment or professional activities. Therefore, the above Regulation becomes inspirational for competition authorities to discern the subjective factors related to the private sphere that could later interfere with consumers' economic decisions, e.g., online shopping or bargaining.

Finally, Regulation 2016/679 clarifies the meaning of 'enterprise' and 'group of undertakings',[47] offering the right to an effective judicial remedy against a data supervision authority[48] and the right to compensation from the data controller or processor for damages.[49] Article 83 provides for fines for undertakings of up to 2% or 4% of their worldwide annual turnover of the preceding financial year in cases of infringement related to personal data processing, including lack of consent.

4 Informed Consent

An earlier report by the European Data Protection Supervisor found that mere silence or inaction in the case of default settings of online social networks or web browsers is not valid consent.[50] It is obvious that prior consent is required before any processing of personal data can occur, and that notice should be given 'in clear and understandable language'. Furthermore, whenever personal information is to be processed, individuals should be entitled to know about it.[51] These recommendations have been included in Regulation 2016/679. In the same vein, 'silence, pre-ticked boxes or inactivity' cannot constitute valid consent. In particular, Recital 32 requires that 'clear affirmative' consent be given with a 'freely given, specific, informed and unambiguous indication' that the individual concerned agrees to data processing. Following this line, ticking a box when visiting a website, choosing technical settings, or another statement or conduct that clearly indicates acceptance of the terms and conditions of privacy, is deemed to pass the test of valid consent. Therefore, informed internet and social media users should avoid ticking any boxes in order to avoid agreeing to unwanted privacy terms. This is because the latter are notoriously very lengthy. As has been suggested, on average, each internet user would need around 244 h a year to read about privacy policies.[52] Similar to hidden

[47] See Article 4(18) and (19) respectively.

[48] See Article 78.

[49] See Article 82.

[50] European Data Protection Supervisor (2014), para. 3.1.4.

[51] Ibid.

[52] McDonald / Cranor (2008), 17; for a similar concern expressed about onerous obligations imposed on consumers when reading often incomprehensible privacy policies, see Kerber (2016), 7.

terms and conditions of sale, statements about personal data processing are concealed in the 'small print'.[53] As the forthcoming case studies will show, most digital giants have construed privacy using rather mysterious terms, such as 'improving customer experience'.

Regulation 2016/679 draws inspiration from Council Directive 93/13/EEC on unfair terms when it requires the controller of personal data to demonstrate 'pre-formulated' consent in 'an intelligible and easily accessible form, using clear and plain language'. Previous experiences with the interpretation of what constitutes 'intelligible' under this Directive have shown the importance of having less sophistication, whenever possible, in privacy terms. However, under Recital 42 of the Regulation, 'informed' consent expects individuals only to be aware of the identity of the controller and of the purposes of personal data processing. This legal innovation is no major overhaul. Knowing the identity of the data processor, or the kind of personal data being processed, does not make an individual immediately aware of all the possible legal consequences of placing trust in a social platform, of browsing, or of downloading software.[54] Similar to the 'take it or leave it' conceptual framework under the law of contract,[55] the Regulation disregards consent whenever an individual has 'no genuine or free choice or is unable to refuse or withdraw consent without detriment'.[56] Popular digital monopolies, such as Google, Facebook, or Microsoft, offer no free choice compared to alternative services, which could be of inferior quality, be it because they are as yet under-developed or less innovative or be it that they are so because such services do not process significant data from their users. Irrespective of what exactly causes a dominant position to come about, there will always be a significant imbalance between a digital monopolist and its users. As Recital 43 of the Regulation rightfully points out, there will be no valid consent 'where there is a clear imbalance', in particular, where personal data has been processed by a public authority. It is then unlikely that consent was freely given. A presumption of lack of 'free' consent will also operate if 'separate' consent cannot be given to different operations of processing. Alternatively, it is possible that consent is required for the performance of a particular service for which data should not be processed at all. Finally, this chapter argues that a modern interpretation of the traditional doctrine of unconscionability of contracts[57] would be welcome in the context of online platforms and could bridge the conceptual divide between the

[53] See the European Data Protection Supervisor (2014), para. 4.3.2.

[54] In the same vein, see Nehf (2016).

[55] See Smith (2005), 12; for the view that the frequency of harsh terms in standard forms of contract is the result of 'the concentration of particular kinds of business in relatively few hands', see Beale (2002), 232; Kessler (1943), 629.

[56] Recital 42 of Regulation 2016/679.

[57] See Bigwood (2003), 247; on the superior bargaining power of monopolists, see Smith (2005), 319; on unconscionability as exploitation, see Smith (2005), 300; Morgan (2015), 211; on the consumers' lack of understanding of privacy policies, see Strahilevitz / Kugler (2016), 20; for the view that informed consent is unrealistic, see Martens (2016), 38.

inequality of bargaining power and the exploitation of weaker and vulnerable consumers.

5 The Case for Competition Intervention Against Targeted Advertising

As mentioned earlier, competition law can address two main categories of anti-competitive practices. For example, it could potentially tackle the sale of personal data by colluding companies and trigger repercussions under Article 101 TFEU and Chapter I of the UK Competition Act 1998. There is some speculative evidence which suggests that data can be worth up to $5000 per person per year to advertisers[58] or up to $8 trillion when including other non-tangible assets.[59] The European Data Protection Supervisor advanced that personal data shared when using online platforms exceeds, by far, €300 billion. It is true that users place trust in internet platforms, thereby contributing to the sharing of their own personal data for free.[60] There is, therefore, a great potential to tackle the sharing of personal data by digital monopolists given the earlier discussion of the forms of acceptable, valid, and informed consent. Both Article 102 (1) (a) TFEU and Chapter II (§18) of the UK Competition Act 1998 refer to the imposition of 'unfair prices' or 'other trading conditions' from which price discrimination could be extracted and unfair terms be inferred.

Earlier attempts to deal with a misuse of data by monopolists failed due to dissenting opinions. The late US Commissioner Rosch had pointed out that Google's power of monopoly or near-monopoly in the search advertising market could be attributed to its 'power over searches', i.e. user data, through deceptive means.[61] However, Commissioner Rosch was sceptical about imposing on monopolists 'a duty to share data' with their rivals.[62] Indeed, such a duty could even run counter to the new data protection framework in the EU. In the US *Google/DoubleClick* merger, the Federal Trade Commission excluded privacy considerations from its analysis.[63] The FTC lacks competence over privacy, and there is no robust but instead only fragmented data protection subject to various pieces of legislation.[64] In

[58] Market Watch, Who Would Pay $5,000 to Use Google? (You), 25 January 2012.

[59] The Wall Street Journal, The Big Mystery: What's Big Data Really Worth? A Lack of Standards for Valuing Information Confounds Accountants, Economists, 12 October 2014.

[60] See also Newman (2014a), 850.

[61] Concurring and Dissenting Statement of Commissioner J Thomas Rosch Regarding Google's Search Practices, In the Matter of Google Inc., FTC File No 111-0163, [2012].

[62] Ibid., 6.

[63] FTC, *Google/DoubleClick*, File No 071-0170, [2007].

[64] See Stigler (1980), 624, who mentioned the Privacy Act of 1974 on the control and access to information about individuals by the federal government; the Fair Credit Reporting Act (1970) or employment laws prohibiting 'the collection or use of sensitive information about sex, race, or

her dissenting opinion, Commissioner Jones Harbour[65] considered the merits of privacy considerations. She rightfully argued that Google/DoubleClick would gain unparalleled access to consumers' data as a result of the merger.[66] The merger has allowed Google to track both users' internet searches and their web site visits. Similarly, Facebook sought to incorporate the information shared by WhatsApp users into its consumer-profiling business model.[67]

The above cases represent missed opportunities to challenge twenty-first century anti-competitive and strategic practices concerning personal data in digital markets. The Sherman Act became law in 1890, the Federal Trade Commission Act in 1914—both antitrust laws are now lagging behind the digital revolution. Objectively, Section 5 of the FTC's Act on unfair and deceptive advertising alone could not have sufficed before the US courts given that a data protection framework is missing from the architecture.[68]

Comparatively, the EU Commission dealt with issues related to data in the *Microsoft/Yahoo!Search* merger case[69] involving the acquisition by Microsoft of Yahoo's internet search and advertising. The Commission considered that a new entrant would have to overcome barriers to entry and, as a result, could incur 'significant costs' associated with developing and updating the search algorithm. The latter would need to have 'a large database'.[70] Although the decision did not consider privacy, it did raise a relevant issue with regard to the transfer of data by advertisers from one system to another.[71] In the *Google/Double Click* merger case,[72] the Commission emphasised the pro-competitive benefits in the form of network effects. These stemmed from serving commercial ads due to the 'large amounts of customer-provided-data' compared to the more limited amounts of data collected by competitors.[73] However, the Commission was not concerned about privacy at this stage; quite the contrary, it went on to mention that the collection of data allowed for 'better targeting of ads' by advertisers.[74] Later, the Commission clarified that DoubleClick does not use behavioural data for the purpose of 'improving ad serving'

physical handicaps'; the Bank Secrecy Act of 1970; the Equal Credit Opportunity Act; Title VII of the Civil Rights Act of 1964; the Genetic Information Nondiscrimination Act etc.

[65] Dissenting Statement of Commissioner Pamela Jones Harbour, In the Matter of *Google/DoubleClick*, FTC File No 071-0170, [2007].

[66] Ibid., 8.

[67] European Commission, Case No. COMP/M.7217 – *Facebook/WhatsApp*, 3 October 2014.

[68] See the efforts of the FTC for ensuring 'Do Not Track' rules for web browsers, data portability, greater transparency, and express consent when collecting sensitive, e.g. health, data, in FTC (2012).

[69] European Commission, Case No. COMP/M. 5727 – *Microsoft/Yahoo!Search Business*, 18 February 2010.

[70] Ibid., para. 111.

[71] Ibid., para. 140.

[72] European Commission, Case No. M. 4731, *Google/DoubleClick,* 11 March 2008.

[73] Ibid., para. 179.

[74] Ibid., para. 182.

to third-party publishers or advertisers.[75] Ultimately, the Commission eventually acknowledged that 'particularly large internet service providers could thus try to team up with advertisement companies to make use of this data under the restrictions imposed by privacy rules, but they could also try to use this data with their customers' consent, for instance in exchange for lower prices'.[76]

While the Commission mentioned the legal framework of privacy rules, it did not thoroughly investigate the economics of privacy, in particular, targeted advertising. It simply assumed that customers could have sufficient bargaining power to extract lower prices.

Another missed opportunity—this time in the UK—of dealing with an alleged online discrimination in the search market for online maps is *Streetmap*.[77] It demonstrates that Google's competitors are having a very hard time proving an 'objective' abuse of dominance[78] on the basis of this monopolist's exclusionary conduct alone, and that it would have been helpful to prove anti-competitive harm to consumers to strengthen the exploitative side of abuse. Apart from this, the High Court of England and Wales stumbled when it refused to admit that, under Article 102 TFEU, there is no *de minimis* doctrine applicable so as to expect an 'appreciable effect in the market for online maps'.[79]

So is it right to believe that privacy is solely a consumer protection issue and not, as yet, a competition law issue? Consumers are often unaware who has access to their personal data; what kind of data is processed; and how, when, and where it is shared or sold.[80] No individual consumer can stand alone in the fight against big data owners. Competition law is, ultimately, the proper solution to online data misuse or abuse.

Critics have argued convincingly that competition law offers a 'convoluted and indirect approach' to online privacy.[81] They have suggested that a unified enforcement of traditional competition and consumer issues could 'destabilise the modern consensus on antitrust analysis', dismissing 'rigorous, scientific methods' to favour 'subjective noncompetition factors'.[82] In sharp contrast, Edelman concluded one of his seminal works on Google with an emphasis upon 'decades-old competition frameworks', which remain 'ill-suited' for fast-moving digital markets.[83]

It is difficult to grasp how an assessment of market dominance will succeed without rigorous economic assessment and why personal data, preferences, and choices

[75] Ibid., para. 182.

[76] Ibid., para. 271.

[77] *Streetmap EU Limited v Google Inc.* [2016] EWHC 253 (Ch) (12 February 2016).

[78] Ibid., para. 56, where the High Court reiterates well-known verses from ECJ, Hoffmann-LaRoche v Commission, C-85/76, ECLI:EU:C:1979:36, para. 91.

[79] Ibid., para. 98; also, see Whish (2016), who clarifies the misunderstanding and subsequently comments on *Streetmap.*

[80] See Grunes / Stucke (2015), 12, who support the view that ignoring privacy as a sole consumer-protection issue is wrong.

[81] Ohlhausen / Okuliar (2015), 156.

[82] Ibid.

[83] Edelman (2015), 397.

should continue to be misused, thereby putting online consumers at an economic disadvantage vis-à-vis sellers or retailers through third-line price discrimination.[84] If consumers are staring at products on display in shops, nobody records their physical presence to later raise the price.[85] Nor do sellers on the high street know how rich their customers are, where they live, and so on. If online privacy continues to be ignored by competition/antitrust authorities in the digital age, then calls will follow shortly to disempower them and empower instead other competent authorities that will, indeed, stand up for online consumers and deal with the culprits of personal data collection, transfer, sharing, or selling. In this author's view, unlike their US counterparts, the EU competition authorities are sufficiently robust and equally flexible to effectively adjust to the needs of the online economy[86] and to successfully protect European citizens as online consumers.

At first glance, the concern over privacy could rightfully be seen as the private affair of a naïve and trusting individual. If there were only one such individual, or just a few, out there, then consumer law would suffice. However, the reality shows that this is not the case. Competition law stands out as a branch of public law[87] and, therefore, it cannot turn a blind eye to the sum of privacy losses by online users at large. The data protection loopholes cannot be taken to provide such a speculative, and thus enriching, ground for large businesses.

A contrary, but commonly held, view dismissing competition policy's intervention in data-driven industries relies on the mutual benefits generally brought by dual-sided platforms for both users and owners. In sharp contrast, the European Data Protection Supervisor has suggested that 'often companies rely on and exploit big data by operating a two-sided or multisided platform or business model, cross-financing distinct services', and that 'these companies compete for the attention and loyalty of individuals whose use of those services will generate personal data with a high commercial value.[88]

Empirical research by economists has suggested that it is uncommon for industries based on two-sided platforms to be monopolies or near monopolies.[89] Yet, the

[84] Under the US antitrust law, this type of price discrimination requires proof of harm to the competitive process, rather than an exploitation of consumers, see Hermalin / Katz (2006), 230.

[85] Also, see Acquisti / Varian (2005), 367, suggesting that, while consumers might be aware of online tracking, firms will be using it to 'tailor prices'; Einav / Levin (2014), 12430894, highlighting inter alia that by knowing behavioural data, i.e. individual preferences, sellers could make pricing changes in response to consumer demand.

[86] In the same spirit, the UK CMA looks confidently to the existing UK and EU competition-law frameworks as being capable of dealing with the abuse of dominance by online platforms; see Competition and Markets Authority (2015), para. 33.

[87] See Chirita (2014), 283.

[88] See European Data Protection Supervisor (2014), para. 2.3.12.

[89] See Evans / Schmalensee (2011), 17, offering several examples, from residential property, securities, TV, media, operating systems, and games to payment cards; on two-sided online advertising, see Rochet / Tirole (2003), 1; on critical features of two-sided markets, such as idiosyncratic matching and inefficient rationing, see Hermalin / Katz (2016).

contrary is held to be the case when it comes to Google's search engine,[90] whose share of the general internet search exceeds 90% of the market. Empirical research on internet search advertising found that this market allows for 'very precise' targeted advertising.[91] Targeted advertising is often associated with privacy intrusion by advertisers,[92] but could also go beyond that to interrupt the online experience of consumers.[93]

Without disregarding the incontestable direct benefits derived by users from Google's online search engine platform,[94] it must be noted that the giant extracts nearly $74.5 billion in revenues, with a 17% increase from advertising.[95] In *Vidal-Hall v Google Inc.*,[96] there is evidence that in 2011, Google extracted $36.5 billion from advertising. Google's mysterious way of gaining profits moves away from a 'magic circle'[97] to a commercial platform where users' searches are returned with featured ads. Advertising is supported by a bulk of data collected from Google's users. This has led Newman to describe Google's advertising as 'a monument to converting privacy into a modern currency (…) based on particular user demographics and backgrounds that the advertiser may be looking for'.[98] Another commentator expressed Google's potential sale of users' data as a privacy derivative, nicknaming it *Googlestroika* to add a public sense of state surveillance.[99] In sharp contrast, two notable commentators regard 'the monetization of data in the form of targeted advertising' as being pro-competitive and not harmful, but rather, 'economically-rational, profit-maximizing behaviour'.[100] However, Evans, who has done pioneering work on 'matching advertising'[101] to consumers, took a more nuanced stance. While the efficacy of online targeted advertising in reducing marketing costs is incontestable, Evans recognised that the collection and analysis of data 'raises

[90] See European Commission (2015), Statement/15/4785, Statement by Commissioner Vestager on antitrust decisions concerning Google, 15 April 2015; Chirita (2015), 115; for the contrary opinion that Google is only dominant in a 'populist', rather than rigorous, antitrust sense, see Wagner-von Papp (2015), 641.

[91] See Rutz / Bucklin (2011); on auction sales of sponsored links in keyword searches, see Edelman / Ostrovsky / Schwartz (2007), 242.

[92] See Tucker (2012), 326.

[93] Ibid., 327.

[94] On search engines as a multi-sided platform, see Hoppner (2015), 356; Lianos / Motchenkova (2013), 419.

[95] Alphabet Investor Relations, Press Release: Alphabet Announces Fourth Quarter and Fiscal Year 2015 Results, 1 February 2016.

[96] Para. 6.1. of the Appendix to the judgement in *Vidal-Hall v Google Inc.* [2015] EWCA Civ 311 (27 March 2015).

[97] Chirita (2010), 111.

[98] Newman (2014a), 3.

[99] Muth (2009), 337.

[100] See Sokol / Comerford (2017), 4; Lerner (2014).

[101] That general advertising to a wider audience has to sort out a 'matching' problem by delivering multiple advertisements to a large number of consumers, see Evans (2009), 43.

difficult issues concerning the expectation of privacy'.[102] The analysis of targeted advertising, which has been made the subject of another economic analysis,[103] has also highlighted the pro-competitive benefits of targeted advertising. However, it has raised the alarm over targeting large amounts of data about consumers. It is believed that targeted advertising will often lead to highly concentrated market structures, such as Google and Facebook.[104] Ultimately, privacy could trigger the enactment of regulations that might be capable, or not, of limiting targeted advertising.[105]

The next section will prove that Google is not alone in engaging in anti-competitive misuse of personal data. First, however, it is argued that the new information economics proves incredibly costly for consumers since online service users possess only imperfect information[106] about the real price to be paid in exchange for the freely available digital platform. This chapter agrees with Stiglitz's theory of economic inequality in the sense that 'increasing information asymmetry feeds increasing economic inequality'.[107] In particular, this author argues that the above-mentioned consumers, through their lack of information about their personal, behavioural, experience, and authentication data with which they pay their dues for the use of online services, perpetuate such economic inequality inflicted through price discrimination. Advertisers increasingly use techniques that target online customers based on data collected from their service partners, namely, individual preferences, physical location, and other characteristics.[108] Ultimately, while targeted advertising increases corporate profits for all platforms, another study points out that consumers could, but need not, become better off.[109]

The challenging side of the data misuse remains that, as the price for data is unknown to online service users, the demand, i.e. service, and supply, i.e. data, curves cannot intersect each other in equilibrium. According to Salop and Stiglitz, in such a scenario, any economic analysis of efficiency becomes pointless.[110] As rightly foreseen by Ohlhausen and Okuliar,[111] it represents a clear departure from the conventional analysis of market price equilibrium. It is advanced that, despite its

[102] Ibid., 38.

[103] Bergemann / Bonatti (2011), 438.

[104] Ibid.

[105] Evans (2009), 52; for the contrary opinion, see Campbell / Goldfarb / Tucker (2015), 47, who demonstrate that privacy regulation could help entrench digital monopolies.

[106] Also, see Tucker (2014), 546, who identifies the need to conduct empirical work on the extent of information asymmetries between consumers and firms in this industry.

[107] Stiglitz (2002), 460, 479.

[108] Newman (2014a), 853 highlighting Google's ascension through similar advertising techniques that rely on Google's available user data.

[109] See Johnson (2013), 140.

[110] Salop / Stiglitz (1982), 1121. Recently, Edelman has developed an economic model suitable for online platforms, suggesting that competition between intermediaries intensifies distortions, see Edelman / Wright (2015), 1283.

[111] Ohlhausen / Okuliar (2015).

legal connotation, privacy denotes all kinds of personal data surrounding a potential buyer, who is misled into accepting a much higher price than the actual, real price that could have been paid if the seller had not known about that data.

Speculations about financial status, preferences, or personal choice offer the seller the chance to raise or lower the price for select categories of buyers. Known as 'data mining',[112] targeted advertising allows sellers to make differential advertising offers to a particular group of customers based on useful correlations derived from their past online behaviour or user location. As has been suggested, it would be useful to study empirically the role of social connections and geographic proximity in shaping preferences and consumer purchasing.[113]

The Wall Street Journal has found evidence to suggest that 'areas that tended to see the discounted prices had a higher average income than areas that tended to see higher prices'.[114] The emerging price discrimination relied on the assumption that poor areas have fewer retail options available locally so that higher prices can easily exploit online retail consumers. This kind of online discrimination experienced by consumers from poorer neighbourhoods has recently been acknowledged by the US Federal Trade Commission.[115] The FTC's report was endorsed by Commissioner Ohlhausen given the impact of big data on 'low-income, disadvantaged, and vulnerable consumers'.[116]

Unfortunately, there remains a persistent research gap in the empirical literature on online price discrimination. In 2015, the UK Competition and Markets Authority usefully commissioned its first research report on the commercial use of consumer data, albeit in selected sectors of the economy, such as motor insurance, clothing retail, and games apps.[117] Although limited in scope, the report attempted to provide insights into consumer data, in particular, personal and non-personal data, such as pseudonymous and aggregate data. It also looked into the ways in which consumer data is being collected, namely, inferred, explicitly declared, or observed through users' interaction. Furthermore, this report sheds light on the current use of behavioural data. A previous study had identified that even 'unstructured' data extracted from individuals' browsing history could reveal relevant economic interests,[118] from which wealth status could also be inferred.

Overall, there are too many data-driven platforms available which are capable of sharing economically relevant data for the purpose of price discrimination. This has recently led one commentator[119] to suggest the emergence of serious accountability issues due to the fact that it will often be impossible to identify any leak of personal

[112] Newman (2014a), 868. See also Newman (2014b), 402.

[113] Einav / Levin (2014), 12430891.

[114] Wall Street Journal, Website Vary Prices, Deals Based on Users' Information, 24 December 2012.

[115] US Federal Trade Commission (2016), 11.

[116] See Separate Statement of Commissioner Ohlhausen (2015).

[117] DotEcon & Analysys Mason (2015).

[118] Einav / Levin (2014), 12430891.

[119] See Nehf (2016).

data. Big corporations like Google, Facebook, Yahoo!, and Microsoft have applied a combination of predictive economics models with sophisticated mechanisms to big data to study individual decisions with reference to key variables.[120] Einav and Levin agree that studying an enormous amount of data increases the likelihood of identifying which ads to show.[121]

Professor Klock critically captures the perils of price discrimination, i.e. 'where one set of consumers is unknowingly paying more for the same product than others', identifying it as 'a clear sign of failure in the marketplace that calls for governmental intervention'.[122]

On the basis of the arguments laid out earlier, this chapter first argues that online price discrimination contributes to higher corporate profits and economic inequality. Second, it argues that competition-policy intervention is therefore needed to reduce this economic inequality that generates a false impression that a few digital giants are competing on the merit of their 'highly innovative' data-driven products and performance. Third, this chapter argues that dominant digital monopolies compete on the basis of a bulk of data collected from their online users that is personal, economically relevant, and sensitive. This innovative IT engineering, which has already won solid corporate profits, should no longer pass unobserved by competition authorities' investigations.

Finally, the negative effects of price discrimination on consumers have recently been acknowledged by the OECD, namely that 'consumers may be increasingly facing a loss of control over their data, and their privacy; they are confronted with intrusive advertising and behavioural discrimination, and are ever more locked-in to the services upon which they rely'.[123]

6 A Comparative Assessment of Case Studies of Privacy

The following section is dedicated to exploring how privacy policies work in practice for consumers of online products or services. In the economic literature, it has already been advanced that there is no empirical basis which could demonstrate that 'large online platforms are likely to collect more data', including more sensitive data,[124] than their smaller counterparts. This section seeks to investigate the privacy policies of four major online platforms, namely, Microsoft, Google, Facebook, and Linked-In. It will primarily focus on the categories of data being collected, the sharing of such data, consent, and disclosure. As during the writing of this chapter it became clear that smaller competing online platforms were also important, Instagram, Snapchat and Whisper are also included. Based on no criterion other

[120] Einav / Levin (2014), 12430896.

[121] Ibid., 12430895.

[122] See Klock (2002), 317.

[123] OECD (2016), 29.

[124] See Lerner (2014), para. 85.

than this author's personal preference, Google tops the table below, which presents an overall picture of the findings.

Privacy policies	Collected data	Data sharing with	Disclosures	Consent
Google	(i) **Personal data** until June 2015 & **personal search queries**; (ii) **Behavioural** data; (iii) **Experience** data, i.e. cookies, Google Analytics tracking via DoubleClick; (iv) **Economically relevant** data, i.e. interactive advertising;[a] (v) **Unique device identifiers** • Authentication	**Third parties**: (i) Companies, organisations or individuals; (ii) **Aggregated data** with publishers, advertisers, or connect sites.	(a) Meeting legal requirements or a governmental request; (b) Investigating violations; (c) Detecting or preventing fraud, security or technical issues; (d) Protecting own interests or that of its users.	Required. **Opt-in** for (i) Sensitive personal data; (ii) Combining DoubleClick cookies with personal authentication.
Microsoft Windows 10	(i) **Personal** data until Jan. 2016; (ii) **Behavioural** data; (iii) **Experience**, i.e. cookies, incl. targeted advertising; (iv) **Device-specific** (IT) • Authentication	(i) **Third parties** until Jan 2016; (ii) Controlled affiliates, subsidiaries, vendors.	(a) Legal disclosure; (b) Users' protection against spam, fraud; (c) Its own security interests.	Required. **Opt-out** for 'interest-based advertising'.
Facebook	(i) **Personal** data; (ii) **Experience** and **usage data**, i.e. visualised content, personal engagement, user frequency, and duration; (iii) Specific **location data**; (iv) **Behavioural data** from third party advertisers through 'relevant ads on and off' service.	(i) Companies that are part of Facebook; and (ii) Integrated third party apps, websites or other services, including third party advertisers.	(a) Legal request, i.e. search warrant, court order, or subpoena; (b) Where the law so requires, incl. from jurisdictions outside of the US; (c) Detecting, preventing, and addressing fraud or other illegal activity; (d) Its own protection or that of others; (e) Preventing death or imminent bodily harm.	**Permission required** for sharing personally identifiable data with third party advertisers or analytics partners; **No consent** for: (i) Targeted advertising and aggregated data transfer, i.e. age, sex, location, and personal preference, to vendors, service providers, and business partners; (ii) Transferring personal data to countries outside the EEA.

(continued)

Privacy policies	Collected data	Data sharing with	Disclosures	Consent
Instagram	(i) **Personal data;** (ii) **Analytics** of personally non-identifiable **data**, i.e. traffic, usage, interactions; (iii) **Experience data**, i.e. cookies, local storage; (iv) **Behavioural data**, i.e. serving ads; (v) **Location data**, incl. unique device identifiers; (vi) **Aggregated data**, i.e. total number of visitors, traffic, and demographic patterns.	(i) Personal, experience, local, and behavioural data with **businesses that are legally part of the same group** and its affiliates; (ii) Experience and location data with **third parties**; (iii) **Anonymised data** for targeted advertisements and **aggregated data** with **others.**	(a) In response to a legal request, i.e. search warrant, court order, or subpoena; (b) When the law so requires; (c) Detecting, preventing, and addressing fraud and other illegal activity; (d) Protecting itself and its users; and (e) Preventing death or imminent bodily harm.	**Consent** for (i) Renting or selling data to third parties; (ii) Transferring personal data to another jurisdiction.
Linked-In	(i) **Personal** data; (ii) **Experience** data, i.e. cookies; (iii) **Behaviour** data, i.e. targeted advertising; (iv) **Inferred** and **aggregated** data. (v) **Location** data.	(i) **Affiliates**; (ii) **Third parties**, i.e. publishers and advertisers; No renting or selling of personal data.	(a) Where permitted by law; (b) Reasonably necessary to comply with a legal requirement; (c) Compulsory disclosures; (d) Responding to claims of violations; (e) Its own interest or that of its users.	(i) **Presumed consent** for service functionality; (ii) **Separate permission**, i.e. **opt-in consent** for personal use of cookies by third party advertisers and ad networks; (iii) **Opt-out** from target advertising only, but not from general advertising; (iv) **Presumed consent**, i.e. express and voluntary acceptance of its user agreement.

(continued)

Privacy policies	Collected data	Data sharing with	Disclosures	Consent
Whisper	(i) **Usage data;** (ii) **Location data**; (iii) **Behavioural data** to personalise user's experience; (iv) **Device-specific data**, i.e. unique device identifier; (v) **Experience data**, incl. previous URLs.	(i) **Other users** and **the public**; (ii) Other **nearby users** location data; (iii) **Vendors**, **consultants,** and other **service providers**; (iv) As a result of M&A; (v) Current and future **affiliates**, **subsidiaries,** and other companies; (vi) Third parties: **aggregated data**.	(a) In good faith, where it is necessary to comply with a law, regulation, legal process, or governmental request.	(i) With consent, i.e. location; (ii) No consent for **behavioural or aggregated data**, incl. for analytics and advertising. (iii) **Opting out** of having web browsing used for behavioural advertising. (iv) On Android, mobile, 'Limit Ad Tracking' feature to **opt out of interest-based ads**.

[a]Cookies are small text files placed on users' devices to help Microsoft collect data and store its users' preferences and settings, to facilitate signing in, provide targeted advertising, combat fraud and analyse service performance

6.1 A Classification of the 'Big Data' Collection

This chapter proposes the following classification of big data on the basis of a comparative analysis of the data collected by multi-sided online platforms. First, this chapter argues that behavioural, usage and content, experience, technical, and location data are all sub-categories of personal data, albeit indirectly, compared to more direct, or highly sensitive, personal data. Aggregated data belong to the category of data inferred from any of the above. Second, the chapter wishes to advance that there is a real danger stemming from the abuse of objectively established commercial justifications of improving security, functionality, or service experience through recent attempts to authenticate users for targeted advertising. The latter fully exploits users' economic behaviour and trust, and their lack of specific knowledge and awareness. Third, this chapter recognises exploitative abuse based on behavioural economics as a competition issue while viewing other types of abuse as belonging to consumer law. The author also recognises that economists could still be irritated by the third proposition, as they need to look at all the complexities of a case, and in doing so, they rarely consider the artificial division of competition, consumer, or data protection laws. In the same spirit, a recent EU soft-law communication acknowledges that online platforms are incredibly complex, being subject to

competition and consumer law, personal data and marketing law, and to the Digital Single Market's freedom for 'data-driven innovation'.[125]

6.1.1 Direct Personal Data

Up until January 2015[126] and June 2015,[127] Microsoft and Google collected personal data from their users of Windows 10 and the search engine, respectively, such as name and email. However, Google encrypts many of its services, restricting access to personal data to its own employees, contractors, and agents only. Linked-In collects personal data, such as email address book, mobile device contacts, or calendar, in order to offer its users a 'personalised and relevant experience'. Facebook collects personal data used by its users for registration purposes. Owned by Facebook since September 2012, Instagram also collects personal data, i.e. email address. Surprisingly, Snapchat collects personal data comprising email address, phone number, and even date of birth. Only Whisper does not collect personal data, as a username is different from the user's real name.

6.1.2 Highly Sensitive Personal Data

Google claims that it did not use cookies or similar technologies for sensitive data, i.e. race, religion, sexual orientation, or health. However, its users cannot disable cookies if Google's services are to function properly.

6.1.3 Behavioural Data

Microsoft collects behavioural data, such as users' preferences and interests, while Google collects similar data, which could reveal 'more complex things' and have an economic significance, i.e. most useful ads, people who matter most, or 'likes' for YouTube videos. Similarly, Linked-In collects behavioural data 'to learn about' its users' interests, while Whisper collects the same data[128] so as 'to personalize user experience'.

---

[125] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Online Platforms and the Digital Single Market COM (2016) 288/2, paras 5 and 11.

[126] See Microsoft's Privacy Statement of January 2015; recent updates are available at: https://privacy.microsoft.com/en-GB/updates.

[127] See Google's Privacy Policy of 30 June 2015 available at: https://www.google.com/policies/privacy/archive/20150630/; recent updates are available at: https://www.google.com/policies/privacy/.

[128] The data includes time, pages, whispers viewed, and interactions.

6.1.4 Content and Usage Data

Microsoft collects usage data, such as browsing and search history, while Google collects logging data about how often users made use of its search engine and their own personal search queries. In addition, Google now stores personal data from its users' browser, including HTML, and application data caches. Even more invasive of its users' privacy is the fact that Google combines personal data from one of its multiple innovative services with that from another. Likewise, Facebook collects the content provided when individuals use its service, including any messages and communications, the location and data of a photo, and usage data, such as the types of visualised content, personal engagement, frequency, or duration.

According to its privacy policy as of January 2013, Instagram collects content data, i.e. photos, comments, and communications, and usage data, including browsing. The latter are passed on to third parties to 'personalize' content and ads. Instagram uses third-party analytics to measure service traffic and usage trends, like URLs, number of clicks, interactions, and viewed pages. However, Instagram claims that its analytics data are not used to identify a particular user. Snapchat also collects usage data, namely, social interactions, communications, messages, and content. According to its latest privacy policy of March 2016, Whisper collects usage data, i.e. content, publicly available replies and chat messages, and interactions.

6.1.5 Technical versus Authentication Data

Microsoft, Google, and Snapchat collect device-specific data, while Facebook collects device identifiers. However, while Microsoft collects IT data about device configuration, Google collects more comprehensive data, including the operating system, unique device identifiers, mobile network, and phone number. Since March 2016, Google associates the unique device identifier or phone number with a user's account. Likewise, Linked-In, Instagram, Snapchat, and Whisper collect mobile device identifiers for data authentication, which for Snapchat includes advertising and unique device identifiers.

6.1.6 Location Versus Authentication Data

Microsoft and Google collect location data. However, Google collects data that can uniquely identify a user's actual location, such as IP address, GPS, Wi-Fi access points, and mobile towers.[129] In contrast, Linked-In collects location data for targeting its users with local jobs or for the purpose of fraud prevention and security. Facebook, Instagram, and Snapchat collect location data, including specific

[129] Users' identification through cookies applies to many of Google's innovations, such as Places, Travel, Product Search, Chrome, Maps, Scholar, YouTube, Talk, Gmail, Google+, Android, etc.

(Facebook) or precise (Snapchat) location data. Finally, Whisper collects past and present location data or at least an approximate geographic location.

But why would anyone track users' locations? In the US *re Aaron's, Inc.* case,[130] the franchisees of a rent-to-own dealer of leased computers used computer software to track customers' locations, capture webcam images, and activate keylogging software to steal login credentials for email accounts and financial and media sites. Evans suggests that, compared to larger companies, individuals browsing from home are most exposed to targeted advertising, as they maintain a unique IP address over time.[131] Bergemann and Bonatti have advanced an insightful economic model of profitability based on IP address tracking by online advertisers.[132]

6.1.7 Objectively Justifiable Personalised Service Experience Versus Authentication Data

The majority of the corporations under review, namely, Microsoft, Google, Linked-In, Snapchat, and Whisper, collect experience data, store users' preferences and settings and, purportedly, authenticate them for fraud detection. Microsoft last updated its privacy policy in January 2016. It now claims to collect data to operate effectively and provide its users with the best service experience. While the latter purpose is entirely and objectively justifiable, Microsoft aims not only to improve but also to personalise its users' experience. The latter seems problematic, as any attempt to personalise data will, in turn, compromise privacy.

Google collects cookies, which uniquely identify its users' browser, local web storage, and data caches. At first glance, this is objectively justifiable for improving services for users, by showing them more relevant search results or making the sharing with other users quicker and easier. For this purpose alone, Google collects a vast array of information that figures out 'basic stuff', e.g. language spoken. However, there are blurred boundaries between improving users' experience and authenticating them. Apart from this, Google pursues its own objective commercial interests: to provide, maintain, protect, and improve its services and develop new ones, and to protect its own users. Similarly, Linked-In collects objectively justifiable data from users to improve their experience and increase their security. Instagram collects experience data, including local storage. Snapchat collects unique advertising identifiers about its users' online activities. However, it claims that such data is used to monitor and analyse trends and usage and to personalise the service. Finally, Whisper uses similar tracking technologies, including the URL a user visited before navigating to its service.

The recent Report of the German Monopolies Commission arrives at a similar conclusion, namely, that social platforms of this kind display an incentive to acquire

[130] FTC, *Re Aaron's, Inc.*, No. C-4442 [2014], available at: https://www.ftc.gov/enforcement/cases-proceedings/122-3256/aarons-inc-matter.

[131] See Evans (2009), 42.

[132] Bergemann / Bonatti (2011), 438.

larger amounts of personal data.[133] This goes beyond what is objectively necessary for ensuring the proper functioning of the platforms.

6.1.8 Targeted Versus General Advertising

Microsoft uses personalised data to help make commercial ads more relevant to its users. Google's privacy policy of March 2016[134] acknowledges that the corporation collects usage data about its own advertising services, such as views or interactions with commercial ads. Most importantly, through cookies, Google also stores economically relevant data about its users' interaction with the advertising services offered by Google's partners or features that may appear on other sites. Analytics data is corroborated with advertising services using DoubleClick to generate further data about visits to multiple sites. Google Analytics is yet another powerful tool for businesses and site owners to analyse the traffic to their websites and apps.

Similarly, Linked-In collects behavioural data to 'serve' general advertising, through various advertising technologies, including web beacons, pixel tags, or cookies. Furthermore, Linked-In makes use of targeted advertising based on its users' public profile or inferred data; usage, including search history, content read, activity followed, participation in groups, pages visited, and so on; and, most importantly, third parties, such as advertising partners, publishers, and data aggregators**.** More specifically, advertisers receive the URL of a user's current page when the user clicks on an ad.

Facebook collects behavioural data from third-party advertisers when its users visit or use third-party websites or apps or when they interact with third-party partners. Facebook aims to improve its advertising to existing users to show them 'relevant ads on and off' its service and to measure the effectiveness and reach of such ads. Instagram uses similar technologies 'to serve ads' by advertisers and other partners.

6.1.9 Written Email and Voice Data

The following 'reassuring' disclaimer, which is used by Microsoft, is actually worrying: 'we do not use what you say in email, chat, video calls or voice mail, or your documents, photos or other personal files to target you'. However, Google collects data about the time, date, and duration of calls. Paragraph 1.8 of Linked-In's privacy policy on the use of cookies assumes that, by visiting its service, users consent to the placement of cookies and beacons not only in their browser, but also in HTML-based emails. A recent empirical study has proved how invasive of privacy is the automated email content analysis by Facebook, Yahoo, and Google.[135]

---

[133] German Monopolies Commission (2015).

[134] Available at: https://www.google.com/policies/privacy/archive/20160325/.

[135] See Strahilevitz / Kugler (2016), 20.

6.1.10 Aggregated Data

For commercial purposes, Instagram monitors metrics, such as total number of visitors, traffic, and demographic patterns, i.e. aggregated data. This is in contrast to diagnosing or fixing technology problems. Also, Google shares aggregated, non-identifiable, data publicly and with third parties, such as publishers, advertisers, or connected sites. Facebook shares with third parties data about the reach and effectiveness of their advertising as well as aggregated data. For example, Facebook passes on to third parties data about the number of ad views or demographic data based on its users' age, sex, location, and personal preference. However, Facebook transfers such data to vendors, service providers, and business partners in order to measure the effectiveness of their ads. Instagram also shares aggregated data which can no longer be associated with a particular user**.** Similarly, Snapchat shares aggregated or 'de-identified' data with third-party advertisers. Finally, Whisper shares aggregated data with vendors, consultants, and other service providers.

6.2 Data Sharing

Data sharing is possible both inside and outside of an online platform. The former could be as harmful as the latter in the case of a merger or acquisition.

6.2.1 Inside Sharing of Data

Most corporations share personal data with their controlled affiliates (Linked-In, Whisper) and subsidiaries (Microsoft, Whisper), other companies that are part of the same group (Facebook, Instagram, and Snapchat), or under common control and ownership (Snapchat). Logically, Instagram shares personal content and usage, experience, and local and behavioural data with Facebook. Snapchat shares similar data with the Snapchat family of companies.

6.2.2 Outside Sharing of Data

Until January 2016, Microsoft shared its users' personal data with third parties, including vendors. Google did the same with third-party companies, organisations, or individuals. Linked-In shares personal data with third parties, while Facebook shares service content, like posts or shares, with integrated third-party apps, websites, or other services, including advertisers. Instagram shares experience and location data with third parties. It shares anonymised data with third parties in order for them to deliver targeted advertisements. Similarly, Snapchat shares personal data with third parties, which may include service providers, i.e. for quality of service;

sellers, i.e. providing goods; and partners, i.e. functionality of service, or as a result of a merger or acquisition. Snapchat users themselves provide personal data to third parties simply by clicking on their links or search results. Third parties may use personal data collected by Snapchat to deliver targeted advertisements, including third-party websites and apps. Whisper also shares similar data with the public. Furthermore, the recipient of a chat message could share its content with others. Location data is shared with other nearby users.

On the basis of the above, this chapter identifies that data sharing with third parties, mostly advertisers, is common practice. Linked-In is the only platform to have published a rather obvious disclaimer according to which it does not 'rent or sell' personal data that its users have not posted on Linked-In.

6.3 Consent

6.3.1 Subject to Consent

Microsoft and Google claim to share personal data subject to their users' consent. Linked-In shares similar data subject to consent in order to carry out instructions by users, provide functionality, protect consumer rights, or comply with laws. Surprisingly, Instagram claims to not 'rent or sell' data to third parties without its users' consent, while Snapchat collects with-consent phonebook data and photos. Whisper also shares with-consent location data.

6.3.2 Opt-In (Explicit) Consent

Microsoft users are already signed up to receive targeted advertising without any prior consent. Google requires opt-in consent for sharing sensitive personal data. As of March 2016, Google requires opt-in consent for combining DoubleClick with personally identifiable data. Likewise, Linked-In requires 'explicit' opt-in consent for personal data collected directly by third-party advertisers through cookies.

6.3.3 Presumed Consent

Linked-In presumes that valid consent has been given to the use of beacons and other advertising technologies. It assumes that, by providing personal data, Linked-In users have 'expressly and voluntarily' accepted the terms and conditions of its Privacy Policy, thereby 'freely accepting and agreeing' to such data processing. One disclaimer mentions that supplying any information deemed to be sensitive by applicable law is entirely voluntary. Another disclaimer warns Linked-In users not to become members if they have any concerns about providing data.

6.3.4 Explicit Consent or Special Permission

Google promises its users not to reduce their rights under its current privacy policy without their explicit consent. But isn't it too late to get such consent, since Google has already collected plenty of information about its users, namely, usage data, preferences, messages, photos, videos, browsing history, map searches, documents, and other Google-hosted content? Under these circumstances, could it still be argued that raising awareness about Google's search engine and educating its users as consumers about their online behaviour would suffice to address the abuse of data with given, but less informed, consent? Most users can barely understand the legal implications of such explicit consent.

Linked-In requires 'separate permission' for sharing personal data with third-party advertisers or ad networks for advertising. Facebook requires similar permission for sharing personally identifiable data, i.e. name or email address, with third-party advertisers or measurement or analytics partners.

6.3.5 Opt-Out Choice

Microsoft offers an 'opt-out' choice, directing its users to visit Microsoft's opt-out page. According to Linked-In's privacy policy of October 2014,[136] in particular, its second commitment, 'If you wish to not receive targeted ads from most third-party companies, you may opt-out by clicking on the AdChoice icon in or next to ad'. However, according to its third commitment, 'This does not opt any user out of being served advertising.' Linked-In's users are empowered to opt out of targeted ads only. They can opt out if they no longer wish their online behaviour to be tracked on third-party sites. Whisper users, in contrast, can opt out of having their web-browsing information used by participating companies for behavioural advertising purposes. On Android mobile, users have to choose the 'Limit Ad Tracking' feature to opt out of interest-based ads.

6.3.6 No Consent

Obviously, no consent is required from Linked-In for its users' public posts. In contrast, Whisper does not require consent for sharing behavioural or aggregated data with third parties, including for analytics and advertising.

Apart from this, there is further scope for trouble because Linked-In processes personal data outside the country where its users live. Facebook may also transfer personal data to countries outside the European Economic Area. Likewise, Instagram and its affiliates or service providers may transfer personal data across borders to another jurisdiction with different data protection laws. Snapchat may also transfer personal data to jurisdictions other than the United States.

[136] An updated version is available at: https://www.linkedin.com/legal/privacy-policy.

Finally, this chapter identifies as common practice users agreeing to give consent on a 'take it or leave it' basis, without having any viable alternative to the use of cookies. Otherwise, the service in question could not work properly.

6.4 Disclosure of Data

The most commonly known ground for outside disclosure is when personal data is necessary to comply with any applicable law (Microsoft, Google, Whisper), rule or regulation (Google, Snapchat, Whisper); requirement or valid legal request (Instagram, Snapchat), such as a search warrant (Facebook, Instagram), civil or criminal subpoenas (Linked-In, Facebook, Instagram), court orders (Facebook, Instagram) or other compulsory disclosures (Linked-In) or to respond to a valid legal process (Facebook, Whisper) from competent authorities, including from law enforcement or other government agencies (Microsoft, Google, Whisper) and from jurisdictions outside of the United States (Facebook, Instagram); in good faith, where it is permitted by law (Linked-In); for the investigation of potential violations (Google, Linked-In, Snapchat); to enforce a privacy policy or user agreement (Linked-In); to protect customers by preventing spam (Microsoft, Google) or to detect or address fraud (Microsoft, Google, Facebook, Instagram, Snapchat); to prevent loss of life or serious injury (Microsoft); to prevent death or imminent bodily harm (Facebook, Instagram); to operate and maintain product security (Microsoft, Google), for technical issues (Google), or safety (Snapchat); and to protect its own rights and property (Microsoft, Snapchat), interests, and users (Google, Linked-In, Facebook, Instagram, Snapchat) or the public (Google).

Finally, Instagram uses an alarming disclaimer that states that it cannot ensure the security of any transmitted information or guarantee that such information is not accessed, disclosed, altered, or destroyed.

7 A Response from Practice: *Vidal-Hall v Google Inc* [2015] EWCA

In *Vidal-Hall v Google Inc*,[137] the claimants did not consent to the use of cookies on their Apple Safari browser. Advertisers used aggregated data about the claimants' browsing experience to target them via the DoubleClick advertising service. As a result of this targeted advertising, personal data was shared with third parties. On appeal, the Royal Court of Justice established a tortious liability for 'misuse of private information'. Similar to this chapter's proposal of abuse of personal data by digital monopolists, *Vidal-Hall v Google Inc.* has significant implications for the

[137] *Vidal-Hall v Google Inc.* [2015] EWCA Civ 311 (27 March 2015); on appeal from the High Court (QB) The Hon Mr Justice Tugendhat [2014] EWHC 13 (QB).

misuse of personal data through the online browsing activities of individuals. While the Court welcomed the possibility of awarding damages for distress in the absence of proof of a pecuniary loss, civil litigation of this kind demonstrates the risks to the consumer and to data protection laws if they are left unaddressed by competition policy intervention. The tortious measure could do justice solely in individual lawsuits.

This case represents a landmark ruling. It recognised the 'misuse of private information' as an 'invasion of privacy'.[138] Unfortunately, when it interpreted Directive 95/46/EC, the Court suggested that the Directive aims to protect 'privacy rather than economic rights'.[139] The same could be said about the reference to the misuse of 'private information', rather than of personal data. The High Court's Justice Tugendhat had previously recognised that browsing information is, indeed, personal data, and that it could have the potential to identify the claimants 'as having the characteristics to be inferred from the targeted advertisements by third parties viewing the claimants' screens'.[140]

The Royal Court of Justice recognised that 'web traffic surveillance tools make it easy to identify the behaviour of a machine, and behind the machine, that of its user'.[141] The Court went on to distinguish between two categories of personal data: on the one hand, direct personal data, including detailed browsing histories, and on the other, the data derived from the use of the DoubleClick cookie.[142] As the latter includes a unique identifier, indirectly inferred data could have enabled the former, i.e. direct personal data, to be linked to an individual device user. In the Appendix to this ruling, there is evidence of the wealth of personal data collected by Google via DoubleClick, including economically relevant data, such as shopping habits, social class, and financial situation, but also many others, like racial or ethnic origin, health, or sexual interests.[143] Unfortunately, Safari browsers have no 'Opt Out' cookies available that would enable their users to sign off from tracking and targeted advertising.

The Court considered that 'targeted advertising is inevitably revelatory as to the browsing history of a particular individual'.[144] Given the limited appetite for awarding an 'extremely high' figure of damages for distress, i.e. £1.2 million, LJ McFarlane dismissed the appeal to the Supreme Court. The ruling also followed the US developments in private litigation. The FTC had settled with Google a civil penalty of $22.5 million because of the misrepresentation to users of the Safari browser that it would not use cookies or serve targeted advertisements to them.[145]

---

[138] Ibid., paras 19 and 23 for the recognition that courts of equity have afforded protection from the misuse of private information via breach of confidence.

[139] Ibid., para. 77.

[140] Ibid., para. 111.

[141] Ibid., para. 114.

[142] Ibid., para. 115.

[143] Ibid., para. 8.1. to 8.4.

[144] Ibid., para. 128.

[145] Ibid., para. 140.

8 Conclusions

The above study of the privacy policies operated by some digital companies has revealed the many inter-related purposes of the collection and processing of the various categories of personal data. It identified that digital giants have, indeed, pursued nearly identical business models based on corporate gains from targeted advertising and exploitation of consumers as online users of a particular service platform. Indeed, the processing of certain categories of data is objectively justifiable for making the service in question work better for its users. However, other categories of usage, content, and behavioural data tend to be rather excessively processed for the benefit of commercial advertising by third parties. Knowing a consumer's usage, frequency, preferences, and choices builds up a picture of their prospective economic behaviour. It disempowers such online consumers from any natural status of rational buyers while making them more vulnerable vis-à-vis online sellers or retailers. Giving consent and opting in or out remain useful compliance tools for corporations that seek to stay safe from data protection rules. But can they also remain so before competition authorities?

References

Acquisti, A. / Varian, H.R. (2005), Conditioning prices on purchase history, 24 Marketing Science, 367-381

Albors-Llorens, A. (2014), Competition and Consumer Law in the European Union: Evolution and Convergence, 33 Yearbook of European Law, 163-193

Armstrong, M. / Vickers, J. (2001), Competitive Price Discrimination, 32 The RAND Journal of Economics, 579-605

Baker, J.B. (2003), Competitive Price Discrimination: The Exercise of Market Power without Anticompetitive Effects, 70 Antitrust Law Journal, 643-654

Barr-Gill, O. (2012), Seduction by Contract: Law, Economics, and Psychology in Consumer Markets, Oxford University Press

Beale, H. (2002), Legislative Control of Fairness: The Directive on Unfair Terms in Consumer Contracts, in: J. Beatson / D. Friedmann (Eds.), Good Faith and Fault in Contract Law, Oxford Clarendon Press

Bellamy and Child (2013), European Union Law of Competition, in: V. Rose / D. Bailey (Eds.), 7th ed., Oxford University Press

Bergemann, D. / Bonatti, A. (2011), Targeting in advertising markets: implications for offline versus online media, 42 The RAND Journal of Economics, 417-443

Bergemann, D. / Brooks, B. / Morris, S. (2015), The Limits of Price Discrimination, 105 American Economic Review, 921-957

Bigwood, R. (2003), Exploitative Contracts, 1st ed., Oxford University Press

Campbell, J.D. / Goldfarb, A., / Tucker, C. (2015), Privacy Regulation and Market Structure, 24 Journal of Economics & Management Strategy, 47-73

Chirita, A.D. (2010), Undistorted, (Un)fair Competition, Consumer Welfare and the Interpretation of Article 102 TFEU, 33 World Competition Law and Economics Review, 417-435

Chirita, A.D. (2014), A Legal-Historical Review of the EU Competition Rules, 63 International & Comparative Law Quarterly, 281-316

Chirita, A.D. (2015), Google's Anti-Competitive and Unfair Practices in Digital Leisure Markets, 11 Competition Law Review, 109-131

Cooper, E.H. (1977), Price Discrimination Law and Economic Efficiency, 75 Michigan Law Review, 962-982

Drexl, J. / Hilty, R. / Desaunettes, L. / Greiner, F. / Kim, D. / Richter, H. / Surblytė, G. / Wiedemann, K. (2016), Data ownership and access to data position statement of the Max Planck Institute for Innovation and Competition, Max Planck Institute for Innovation and Competition Research Paper No. 16-10, available at: http://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/positionspaper-data-eng-2016_08_16-def.pdf

Edelman, B. (2015), Does Google Leverage Market Power through Tying and Bundling, 33 Journal of Competition Law and Economics, 365-400

Edelman, B. / Ostrovsky, M. / Schwartz, M. (2007), Internet Advertising and the Generalized Second-Price Auction: Selling Billions of Dollars Worth of Keywords, 97 American Economic Review, 242-259

Edelman, B. / Wright J. (2015), Price Coherence and Excessive Intermediation, 130 The Quarterly Journal of Economics, 1283-1328

Einav, L. / Levin, J. (2014), Economics in the Age of Big Data, 346 Science, 12430891-12430896

Evans, D.S. (2009), The Online Advertising Industry: Economics, Evolution, and Privacy, 23 Journal of Economic Perspectives, 37-60

Evans, D.S. / Schmalensee, R. (2011), The Industrial Organization of Markets with Two-Sided Platforms, in: D.S. Evans (Ed.), Platform Economics: Essays on Multi-Sided Businesses, Competition Policy International, 2-29

Evans, D.S. / Ezrachi, A. (2015), Witness Statement to the House of Lords' Inquiry on Online Platforms and the EU Digital Single Market, available at: https://www.publications.parliament.uk/pa/ld201516/ldselect/ldeucom/129/129.pdf

Grunes, A.P. / Stucke, M.E. (2015), No Mistake about It: The Important Role of Antitrust in the Era of Big Data, 12 Antitrust Source, 1-14

Hayek, F.A. (2002), Competition as a Discovery Procedure, 5 Quarterly Journal of Austrian Economics, 9-23

Heffetz, O. / Ligett, K. (2014), Privacy and Data-Based Research, 28 Journal of Economic Perspectives, 75-98

Hermalin, B.E. / Katz, M.L. (2006), Privacy, Property Rights and Efficiency: The Economics of Privacy as a Secrecy, 4 Quantitative Marketing and Economics, 209-239

Hermalin, B.E. / Katz, M.L. (2016), What's So Special about Two-Sided Markets?, forthcoming in Economic Theory and Public Policies: Joseph Stiglitz and the Teaching of Economics, Columbia University Press

Hoppner, T. (2015), Defining Markets for Multi-Sided Platforms: The Case of Search Engines, 38 World Competition, 349-366

Johnson, J.P. (2013), Targeted advertising and advertising avoidance, 44 The RAND Journal of Economics, 128-144

Joyce, D. (2015), Privacy in the Digital Era: Human Rights Online?, 16 Melbourne Journal of International Law, 1-16

Kadar, M. (2015), European Union Competition law in the Digital Era, 4 Zeitschrift für Wettbewerbsrecht, 342-363

Kerber, W. (2016), Digital markets, data, and privacy: competition law, consumer law and data protection, 11 Journal of Intellectual Property Law & Practice, 856-866

Kessler, F. (1943), Contracts of Adhesion – Some Thoughts about Freedom of Contract, 43 Columbia Law Review, 629-642

Klock, M. (2002), Unconscionability and Price Discrimination, 69 Tennessee Law Review, 317-331

Lerner, A.V. (2014), The Role of 'Big Data' in Online Platform Competition, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2482780

Lianos, I. / Motchenkova, E. (2013), Market Dominance and Quality of Search Results in the Search Engine Market, 9 Journal of Competition Law & Economics, 419-455
Lynskey, O. (2014a), Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order, 63 International and Comparative Law Quarterly, 569-597
Lynskey, O. (2014b), The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: *Digital Rights Ireland*, 51 Common Market Law Review, 1789-1811
Lynskey, O. (2015), Control over Personal Data in a Digital Age: *Google Spain v AEPD and Mario Costeja Gonzalez*, 78 Modern Law Review, 522-534
McDonald, A.M. / Cranor, L.F. (2008), The Cost of Reading Privacy Policies, 4 Journal of Law and Policy for the Information Society, 543-568
Morgan, J. (2015), Great Debates in Contract Law, 2nd ed., Palgrave
Muth, K.T. (2009), Googlestroika: Privatising Privacy, 47 Duquesne Law Review, 337-354
Nehf, J.P. (2016), Protecting Privacy with 'Heightened' Notice and Choice, in: J.A. Rothchild (Ed.), Research Handbook on Electronic Commerce Law, Edward Elgar
Newman, N. (2014a), The Cost of Lost Privacy: Consumer Harm and Rising Inequality in the Age of Google, 40 William Mitchell Law Review, 850-879
Newman, N. (2014b), Search, Antitrust and the Economics of the Control of User Data, 30 Yale Journal on Regulation, 401-454
O'Donoghue, R. / Padilla, A.J. (2006), The Law and Economics of Article 82 EC, 1st ed., Hart Publishing
Ohlhausen, M.K. / Okuliar, A. (2015), Competition, Consumer Protection, and the Right [Approach] to Privacy, 80 Antitrust Law Journal, 121-156
Pasquale, F.A. (2013), Privacy, Antitrust and Power, 20 George Mason Law Review, 1009-1024
Posner, R. (1980), The Economics of Privacy, 71 American Economic Review, 405-409
Roberts, A. (2015), Privacy, Data Retention and Domination: *Digital Rights Ireland Ltd v Minister for Communications*, 78 Modern Law Review, 535-548
Rochet, J.C. / Tirole, J. (2003), Platform Competition in Two-Sided Markets, 1 Journal of the European Economic Association, 990-1029
Rutz, O. / Bucklin, R. (2011), From Generic to Branded: A Model of Spillover Dynamics in Paid Search Advertising, 48 Journal of Marketing Research, 87-102
Salop, S. / Stiglitz, J.E. (1982), The Theory of Sales: A Simple Model of Equilibrium Price Dispersion with Identical Agents, 72 American Economic Review, 1121-1130
Schepp, N.P. / Wambach, A. (2016), Economist's Note on Big Data and Its Relevance for Market Power Assessment, 7 Journal of European Competition Law and Practice, 120-124
Smith, S.A. (2005), Atiyah's Introduction to the Law of Contract, Oxford Clarendon Press
Sokol, D. / Comerford, R. (2017), Does Antitrust Have a Role to Play in Regulating Big Data?, in: R. Blair / D. Sokol (Eds.), Cambridge Handbook of Antitrust, Intellectual Property and High Tech, Cambridge University Press, 293
Stigler, J. (1980), An Introduction to Privacy in Economics and Politics, 9 Journal of Legal Studies, 623-644
Stiglitz, J.E. (2002), Information and the Change in the Paradigm in Economics, 92 American Economic Review, 460-501
Tucker, C. (2012), The economics of advertising and privacy, 30 International Journal of Industrial Organization, 326-329
Tucker, C. (2014), Social Networks, Personalized Advertising and Privacy Controls, 51 Journal of Marketing Research, 546-562
Wagner-von Papp, F. (2015), Should Google's Secret Sauce Be Organic?, 16 Melbourne Journal of International Law, 608-646
Whish, R. (2016), Article 102 and de minimis, 15 Competition Law Journal, 53-58
Whish, R. / Bailey, D. (2015), Competition Law, 8th ed., Oxford University Press

Additional Sources

Alphabet Investor Relations (2016), Press Release: Alphabet Announces Fourth Quarter and Fiscal Year 2015 Results, 1 February 2016, available at: https://abc.xyz/investor/news/earnings/2015/Q4_google_earnings/

Autorité de la concurrence and Bundeskartellamt (2016), Competition Law and Data, available at: http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf

Bundeskartellamt (2016), Press release, Bundeskartellamt initiates proceedings against Facebook on suspicion of having abused its market power by infringing data protection rules, 2 March 2016 available at: https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html

Committee of Economic and Monetary Affairs (2014), Hearing of Margrethe Vestager, 2 October 2014, available at: http://www.europarl.europa.eu/hearings-2014/resources/library/media/20141022RES75845/20141022RES75845.pdf

Competition and Markets Authority (2015), Written Evidence (OPL0055) to the House of Lords' Inquiry on Online Platforms and the EU Digital Single Market, available at: https://www.publications.parliament.uk/pa/ld201516/ldselect/ldeucom/129/129.pdf

DotEcon & Analysys Mason (2015), The Commercial Use of Consumer Data A research report for the CMA, available at: https://www.gov.uk/cma-cases/commercial-use-of-consumer-data

European Commission (2015), Statement by Commissioner Vestager on antitrust decisions concerning Google, 15 April 2015, available at: http://europa.eu/rapid/press-release_STATEMENT-15-4785_de.htm

European Data Protection Supervisor (2014), Preliminary Opinion of the European Data Protection Supervisor, Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf

German Monopolies Commission (2015), 68th Special Report on Competition Policy: Challenges of Digital Markets, available at: http://www.monopolkommission.de/images/PDF/SG/SG68/S68_volltext.pdf

Guardian (2010), Privacy No Longer a Social Norm, Says Facebook Founder, 10 January 2010, available at: https://www.theguardian.com/technology/2010/jan/11/facebook-privacy

London School of Economics (2015), Online Platforms and the EU Digital Single Market, Written Evidence (OPL0054) to the House of Lords, the Select Committee on the European Union, available at: https://publications.parliament.uk/pa/ld201516/ldselect/ldeucom/129/129.pdf

Market Watch (2012), Who Would Pay $5,000 to Use Google? (You), 25 January 2012, available at: http://blogs.marketwatch.com/realtimeadvice/2012/01/25/who-would-pay-5000-to-use-google-you/

Martens, B. (2016), European Commission, Joint Research Centre Technical Reports, An Economic Policy Perspective on Online Platforms, available at: https://ec.europa.eu/jrc/sites/jrcsh/files/JRC101501.pdf

OECD (2016), Big Data: Bringing Competition Policy to the Digital Era, DAF/COMP(2016)14, available at: https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf

Ohlhausen, M.K. (2016), Separate Statement, Big Data: A Tool for Inclusion or Exclusion, 6 January 2016, available at: https://www.ftc.gov/system/files/documents/public_statements/904483/160106bigdatarptmkostmt.pdf

Strahilevitz, L.J. / Kugler, M.B. (2016), Is Privacy Policy Language Irrelevant to Consumers?, Chicago Coase-Sandor Institute for Law and Economics Working Paper No. 776, available at: http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2465&context=law_and_economics

US Federal Trade Commission (2012), Protecting Consumer Privacy in an Era of Rapid Change, March, available at: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-

commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

US Federal Trade Commission (2016), Report on Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues, January, available at: https://www.ftc.gov/system/files/documents/public_statements/904483/160106bigdatarptmkostmt.pdf

Vestager, M. (2016), Competition in a Big Data World, Speech, 18 January 2016, available at: https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/competition-big-data-world_en

Wall Street Journal (2012), Website Vary Prices, Deals Based on Users' Information, 24 December 2012, available at: https://www.wsj.com/articles/SB10001424127887323777204578189391813881534

Wall Street Journal (2014), The Big Mystery: What's Big Data Really Worth? A Lack of Standards for Valuing Information Confounds Accountants, Economists, 12 October 2014, available at: https://www.wsj.com/articles/whats-all-that-data-worth-1413157156

Big Data, Open Data, Privacy Regulations, Intellectual Property and Competition Law in an Internet-of-Things World: The Issue of Accessing Data

Björn Lundqvist

Contents

1 Introduction 192
2 The [Intellectual] Property-Law Regulation of Big Data and Its Ecosystem 194
3 The Definition of Data 198
4 Standards for the Internet of Things, Industrial Internet and IoT Patent Platforms or Pools 201
5 The Application of Competition Law 202
6 Sector-Specific Regulations and Data-Protection Rules 207
7 Conclusion 211
References 211

Abstract The interface between the legal systems triggered by the creation, distribution and consumption of data is difficult to grasp, and this paper therefore tries to dissect this interface by following information, i.e. 'data', from its sources, to users and re-users and ultimately to its consumers in an 'Internet of Things', or 'Industrial Internet', setting. The paper starts with the attempt to identify what legal systems are applicable in this process, with special focus on when competition law may be useful for accessing data. The paper concludes that general competition law may not be readily available for accessing generic (personal or non-personal) data, except for situations in which the data set is indispensable to access an industry or a relevant market, while sector-specific regulations seem to emerge as a tool for accessing data held by competitors and third parties. However, the main issue under general competition law in the data industry, at its current stage of development, is to facilitate the implementation of the Internet of Things.

Dr. Björn Lundqvist, LLM (Michigan) is Associate Professor of EU Law at Stockholm University.

B. Lundqvist (✉)
Stockholm University, Stockholm, Sweden
e-mail: bjorn.lundqvist@juridicum.su.se

M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law*, MPI Studies on Intellectual Property and Competition Law 28, https://doi.org/10.1007/978-3-662-57646-5_8

1 Introduction

The interface between digitalized information (data), intellectual property, privacy regulations and competition law in the 'Internet of Things' (IoT) scenario is currently triggering the interest of politicians, businessmen, the academic community and even the general public. The groups are interested for different reasons; for example, businessmen see an opportunity for the creation of wealth, researchers see the possibility of gaining, analysing and distributing knowledge efficiently and everyone acknowledges that the collection and distribution of personal data may raise both privacy and data-protection concerns.

The interface between the legal systems triggered by the creation, distribution and consumption of data is difficult to grasp, and this paper therefore tries to dissect this interface by following information, i.e. 'the data', from its sources, to users and re-users and ultimately to its consumers in an IoT setting. The sources of data can be very different, but they can be divided into three main groups: firstly, government data ('open data'), i.e. personal or non-personal data collected by public-sector bodies (PSBs); secondly, data can be voluntarily provided by users, consumers or businesses on e-platforms or when using other forms of IT-based services; and thirdly, data can be simply generated, e.g. by cookies, ISP data, eCall data, even patient data.[1] Of course, any data collected can be either personal or non-personal; however, personal and non-personal data is often mixed and combined in data sets, and sometimes when different types of non-personal data are mixed in the same data set, the data can become personal data, since the combination of data might identify and reveal information regarding a person when sophisticated algorithms are used.

The paper starts with the attempt to identify what legal systems are applicable in this process. What intellectual property law system may be applicable when data is obtained from devices and distributed to 'The Cloud', and, ultimately, when it is re-used? Who 'owns' personal data, and do data-protection rules create nascent property rules regarding personal data? Secondly, the paper will discuss when creators, holders and consumers of raw or processed data, either private or public bodies, should benefit from the application of competition law, and whether competition law facilitates the needs that are identified.[2] The paper specifically focuses on the application of competition law vis-à-vis the bodies that collect or hold data. Also, may competition law be used to gain access to open or big data, or the infrastructure around that data?[3] May competition law be used to create a level playing field between holders and non-holders of essential data?

Thirdly, the paper will raise the issue of sector-specific regulation in the arena of data. Access to data is a disputed issue not only under 'general' competition law, but also in reference to sector-specific regulations such as the Public Sector Information

[1] OECD (2015); OECD (2016); Autorité de la Concurrence and Bundeskartellamt (2016). See also regarding open data Lundqvist / Vries / Linklater / Rajala Malmgren (2011).

[2] See Ezrachi / Stucke (2016) and Stucke / Grunes (2016).

[3] In reference to open data see Drexl (2015), 64-100. See also Lundqvist (2013), 79-95.

Directive,[4] the eCall Regulation[5] and in the field of financial services[6] and in reference to e-platforms.[7] Indeed, it seems that rules regarding access to data (*ex ante* regulations) are currently seeping into sector-specific regulations, implying an obligation to either share data or grant open access to the device that collects the data.[8]

The paper concludes that general competition law may not be readily applicable to access to generic data, except for situations in which the data set is indispensable to access an industry or a relevant market[9]; while sector-specific regulations seem to emerge as a tool for accessing data held by competitors or firms in general. However, the main issue under competition law in the data industry, at its current stage of development, is to create a level playing field by trying to facilitate the implementation of the IoT. For example, we might see brick-and-mortar firms develop towards collecting, storing and trading data in competition with the incumbent e-platform firms. Such a development could increase competition in the data industry to the benefit of consumers and society. However, if we can predict that this might happen, what consequences might that have for the use of competition law vis-à-vis the incumbent firms in the data industry, hence those firms, e.g. Google, that have been found or are under investigation for abusing their dominant position.

Finally, there is a great need for IoT standards in general and functional IP rules or guidelines under these standards in particular. When IoT becomes a reality, devices will communicate with other devices, with the telecom technology, and with the cloud. Devices and device producers need rules and guidelines regarding interoperability, otherwise the system may not materialize. If the device industry is to become connected it will also need to deal with standard-essential patents (SEPs) and the issue of FRAND. Indeed, we are at the beginning of the development of everything's interoperability. Perhaps competition authorities should be more cautious vis-à-vis standards consortia and other forms of pre-market collaborations now being set up for the upcoming IoT paradigm—in this context also called the

[4] The Directive on the re-use of public sector information (Directive 2003/98/EC, known as the 'PSI Directive') entered into force on 31 December 2003, [2003] OJ L 345/90. It was revised by Directive 2013/37/EU, which entered into force on 17 July 2013, [2013] OJ L 175/1.

[5] Regulation (EU) 2015/758 of the European Parliament and of the Council of 29 April 2015 concerning type-approval requirements for the deployment of the eCall in-vehicle system based on the 112 service and amending Directive 2007/46/EC, [2015] OJ L 123/77.

[6] In order to accelerate retail banking innovation and simplify payments, the European Commission is mandating standardized API access across the EU. The initiative is part of the European Commission's update of the Payment Services Directive (PSD). The revision of the PSD (PSD2) requires banks to provide access to third parties. See Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directive 2002/65/EC, Directive 2009/110/EC and Directive 2013/36/EU and Regulation (EU) No 1093/2010 and repealing Directive 2007/64/EC, [2015] OJ L 337/35. Cf. Commission (2015).

[7] There are French national initiatives to open e-platforms for third-party competitors. See e.g. French Senate (2013).

[8] Chisholm / Jung (2015), 7-21.

[9] ECJ, Huawei Technologies, C-170/13, ECLI:EU:C:2015:477.

Industrial Internet—than the establishment of dominance in the data industry. Are we seeing signs of firms trying to agree on technical solutions, not so as to facilitate the IoT, but rather to promote their own technical solution while excluding those of others? Some aspects of such conduct might be procompetitive, while other aspects might be anticompetitive. The competition authorities are thus forced to weigh the benefits of such collaborations with their negative impact on competition. Indeed, the legislators' as well as the Commission's effort should be to create a vibrant competitive data industry environment in an IoT setting, but the Commission, and other competition agencies, need to work 'smart' and focus on collaborative and unilateral conduct that is likely to become anticompetitive when it becomes possible to identify the IoT markets.

2 The [Intellectual] Property-Law Regulation of Big Data and Its Ecosystem

The creation, collection, storing, commercially using, and dissemination of data, be it government (open) data and/or private (big) data,[10] require a number of components to materialize. Most importantly, the data industry needs someone who wants to invest in the collection and storing of data. Until lately, a government authority or a similar body has usually been the data collector. Hence, a PSB, based on an obligation in law, collecting necessary data for society concerning, for example, land ownership, trademarks, weather information, maps or company data, and storing the data on servers, has up until recently been the 'normal' data collector. While these public collectors have gradually, voluntarily or under the PSI Directive, begun to market the data to consumers on the Internet and to firms reusing the same (e.g. data brokers, or data re-users), private parties, with few exceptions, have not had the interest or the means to collect and store vast amounts of data in a similar way.[11]

However, with Google, Amazon and Facebook, possibly, being the pioneers, private entities are clearly starting to collect and store a large volume of data, which is mostly personal (consumer) data.[12] Private parties selling ads online, or, more accurately, access to avenues for the marketing of goods or services to potential consumers, have realized that it may be profitable to collect personal data. Mainly consumer data, but also other forms of information and knowledge, are collected. These firms want to be able to sell focused ads or avenues that, with the use of the collected user

[10] The definition of big data is vague and lacks precision; see de Mauro / Greco / Grimaldi (2016), 122-135.

[11] For general information see OECD (2015). For the costs of the necessary investments to access the data industry see OECD (2016).

[12] Google is involved in several investigations in several jurisdictions regarding the company's business conduct; see for example European Commission, Press release (IP/16/1492), Antitrust: Commission sends Statement of Objections to Google on Android operating system and applications, 20 April 2016.

data and algorithms, pin-point the most likely purchasers and also warrant that the commercial message will penetrate, reach and nudge the intended focus groups.[13]

In addition, some firms are today actively seeking out unique data sets, especially in the cultural arena, to gain more traffic in their own ecosystems, thus to collect even more personal data and thereby boost their marketing service vis-à-vis firms wanting to market on-line.[14] Google has, for example, been accused of leveraging its potential market power based on holding vast amounts of data by expanding its business from general search into new services and products, provided to users at zero price, while the goal of these new services or products is to obtain more data from users.[15] Indeed, Google is active on two levels or markets: downstream, providing diversified on-line services to consumers, but also upstream, on the ads market, where the data collected from the zero-price services is used to obtain a competitive edge.

It is clear that, especially Google, but also other e-platforms and ecosystems (for example, Apple, Amazon, Microsoft, Facebook and to some extent Spotify) are in the business of collecting personal data that is either voluntarily provided by users or collected from users based on their conduct, e.g. general and special searches, cookies etc. They collect this data so to profile the users and they can then provide a marketing service to firms which better identifies potential customers and better adapt the message to these customers. Soon, possibly, the data can also be used for predictive modelling, i.e. to enable the message sent to penetrate to and convince the customer what to select even before the customer understand what he or she needs. Moreover, several economists and lawyers have suggested that the collection of personal data causes these firms to gain and hold market power.[16] Indeed, they foresee that the market power obtained by holding vast amounts of data will create insurable barriers to entry for second movers and even that the market for providing services based on data may tip due to indirect network effects based on the holding of vast amounts of data.[17] The amount of data collected increases the quality of the service, which in turn attracts more users to the service.

While these first movers in the data industry may hold market power and are intensively competing to position themselves for the upcoming IoT paradigm, it is clear that the brick-and-mortar industries will start to monitor users and collect data when

[13] Ibid.

[14] See the updated PSI Directive, now including museums, libraries and other cultural institutions, and, moreover, the awkward exemption for exclusive licenses for cultural databases. Cf. The Directive on the re-use of public sector information (Directive 2003/98/EC, known as the 'PSI Directive'), which entered into force on 31 December 2003: [2003] OJ L 345/90. It was revised by Directive 2013/37/EU, which entered into force on 17 July 2013: [2013] OJ L 175/1.

[15] Newman (2013), 3 et seq. with references.

[16] Ibid. See also e.g. Kerber (2016), 3 et seq.

[17] Ibid. See also OECD (2016); Autorité de la Concurrence and Bundeskartellamt (2016), 7, 10 et seq.

everything becomes connected. The brick-and-mortar firms may then try to enter the data industry based on their market position for the specific devices they produce.[18]

What will happen when car manufacturers, refrigerator producers etc. start collecting data based on their products is difficult to predict, but it may cause something similar to 'multi-homing'. Most likely, general or generic consumer data regarding use, data traffic, consumption, GPS position etc., will be collected by several firms. This in turn could lead to increased sale or licensing of data or database connections for the re-use of data, similar to what has happened in the PSI sector. Thus, markets for collection, storing and selling or licensing big-database access will evolve and large brick-and-mortar firms may enter this market in competition with the incumbent Google, Microsoft; Amazon etc.[19]

For brick-and-mortar firms to start collecting data, the infrastructure needs to be in place, at least if we want parties to work themselves up vertically from production of devices and also become the creators and collectors of data sets. Here we see the revolutionary aspect of what we today call the IoT. The IoT essentially comprises client-side devices with different sensors (speed, acceleration, motion, proximity, location, distance, weight, humidity, altitude, depth, compass, temperature, pressure, still image, video image, infrared, audio, noise level, blood sugar, heart rate, number of steps etc.) that are connected to a server side through the Internet. Of course, technically, this is not something entirely new. Previously, the IoT technology was marketed under the concept of M2M (machine to machine). Both devices with sensors and the telecom networks could handle M2M, but M2M did not succeed because of 'back-office' technology problems.[20] The 'cloud', i.e. the servers and the client-server interface, were not up for the challenge. The capacity to, very quickly and inexpensively, store massive volumes of data was not available. This has changed in the emerging IoT era, since computer firms have in the last 10–15 years invested in R&D in the server-client technology and the client-server technology is now mature enough to be implemented.[21] So, what firms will control the client-server interface? According to some studies, the patent distribution in the IoT domain is very fragmented, with the top patent filer in the field holding around 5% of the total patents.[22] Accordingly, LG holds the largest patent portfolio and is closely followed by Ericsson and Qualcomm. Others claim that Microsoft holds the largest portfolio in terms of the client-server interface.[23] Possibly there is, thus, some confusion about whose technology will be used for the IoT standards. Nonetheless, the client-server-interface technology will be protected by patents and, moreover, the upcoming 5G

[18] OECD (2016). Autorité de la Concurrence and Bundeskartellamt (2016), 10 et seq.

[19] Regarding the potential benefits of trading data see Lundqvist (2013), 79-81.

[20] Östman (2016), 1 et seq.

[21] Ibid.

[22] Lexinnova (2014), 3 et seq.

[23] Östman (2016), 1 et seq.

and the current 4G, i.e. the network-infrastructure technology, could even be considered as suffering from early signs of a patent-thicket fatigue.[24]

Thus, the cloud and the interface between devices, 5G telecom and the cloud are the new 'things' in the Internet of Things. A new 'thing' is also the need for technical standards in reference to these interfaces. It is telling to see that CEN and CENELEC are now quickly adopting to the new paradigm and are implementing IP guidelines and SEP policy briefs.[25] Moreover, given the large amount of patents in IoT, we presumably will see several SEP litigations in the future.

For the brick-and-mortar firms to evolve into data-processing firms, they need to develop machine-learning algorithms and also possibly their own clouds. Otherwise, the incumbent firm, such as Amazon, Google and Microsoft, will provide these services and the brick-and-mortar firms will only provide the hardware, i.e. the devices.[26] The industry would then evolve in the direction of more collaborations between the incumbent data firms and the brick-and-mortar firms, and the early signs we see now of high concentration in the data industry could presumably be ascertained depending on whether we would like competition to thrive in the data industry.[27] Indeed, oligopolies, (eco)systems with system leaders, with great interoperability inside the ecosystems, and less or dysfunctional interoperability between the ecosystems will evolve.

Interoperability technologies, like the IoT, promise that devices of everyday life will be able to communicate with each other and that such communication can be stored in the cloud, i.e. in the global data-storing system with increasing capacity. The large capacity can be attributed to client-server technology, and examples of increasing M2M or device-to-device (D2D) communication abound. In the automotive industry, the eCall machines already today open up the possibility of obtaining all sorts of information regarding the car and the driver, while car manufacturers conduct R&D on apps or driverless systems that require multiple connected devices to work together (e.g., sensors, radars, high-powered cameras etc.).[28] Smart cities, smart buildings, smart grids and electromobility converge with mechanical engineering, logistics and seamless wireless communications to

[24] Ibid.

[25] Cf. CEN and CENELEC (2016), 1 et seq.

[26] OECD (2016). Autorité de la Concurrence and Bundeskartellamt (2016), 14.

[27] 'With companies such as Amazon, Google and Microsoft providing machine learning algorithms as part of their cloud computing services, small companies find it increasingly more convenient to have their data processed and mined using external IT infrastructures. Indeed, Cisco forecasts that, by 2019, 86% of all business workload processing will be processed by cloud computing. But, as a greater number of companies become dependent on the infrastructures of a few providers, the latter get access to significant volumes and variety of data that allows them to improve further their own data analysis algorithms. If the trend continues, a competition problem may arise in the future, as new entrants may not be able to build sufficiently powerful IT infrastructures whose analytical software can compete with those of incumbents.', OECD (2016). Autorité de la Concurrence and Bundeskartellamt (2016), 14.

[28] Cf. CEN and CENELEC (2016), 1 et seq.

provide new functionalities for businesses and consumers, including lighting, air quality control, security and surveillance, traffic management etc. Thus, data may be collected and stored as a by-product from all forms of devices and communication, and while the data had a different first use, e.g. to guide the car driver or to communicate between cars, it may be re-used for other purposes.[29]

In reference to the IoT line of thinking, the 'device' industry will be mature industries inhabited by often large firms that have their own IP portfolios.[30] For example, the car is a 'device' in the data industry, and while the intellectual property rights are stacking up in the IoT, the car manufactory industry has a likewise densely populated intellectual property rights landscape.[31]

Indeed, in light of the above, data, originating from users or from devices, sent through the 4G or 5G networks to the client servers and the cloud are heavily boxed in by intellectual property rights. The intellectual property rights cater to the technologies and the infrastructure, while the data as such is probably not covered by the infrastructure intellectual property rights. However, firms holding large IP portfolios in the specific device industry might try to exclude or obtain licensing fees from a new user trying to access data flowing in the system or stored in the cloud connected to the specific device they produce.[32] However, the network providers and the algorithm providers, and possibly also the providers of the specific cloud (if they are separate entities), may also try to either access the data collected by the specific device or even, by technical means, try to exclude others from gaining access to the data. Indeed, even though the data is owned by no one, the firms providing the collection mechanisms, or other vessels, i.e. the devices or platforms for data, have obtained intellectual property rights to these. Presumably, in the end, this will probably require these firms to collaborate.[33]

3 The Definition of Data

According to Article 4 of the General Data Protection Regulation (GDPR), 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an

[29] Ibid.

[30] For an explanation of patent thickets, see Shapiro (2001), 119.

[31] Cf. CEN and CENELEC (2016), 1 et seq.

[32] There are several news articles regarding for example the collaboration/license agreements between Microsoft and Facebook regarding the Microsoft Cloud. Also, users of the Microsoft Cloud need to obtain a license from Microsoft, available at: https://www.microsoft.com/en-us/Licensing/product-licensing/innovations-for-the-cloud.aspx.

[33] See for example Telecommunications and automotive players form global cross-industry 5G Automotive Association, 27 September 2016, available at: https://www.ericsson.com/en/news/2016/9/telecommunications-and-automotive-players-form-global-cross-industry-5g-automotive-association-

identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The definition of personal data is wide since information that is non-personal might also indirectly, in combination with other information, identify a natural person and become personal data. Thus, non-personal, even metadata, can in combination with other data become personal data under this definition. It is therefore recommended that firms collecting data, even only metadata or aggregated data, even in an industrial-internet setting, do take the rules contained in the GDPR into consideration.

An interesting issue is whether the connection or conclusion based on personal data points should be considered personal data, or not. For the upcoming predictive modelling marketing tool and the discussion regarding property right for non-personal data this is important. Indeed, it can be wise to calibrate the collection mechanism, in for example an industrial-internet setting, to only transfer and collect non-personal data, which can be conclusion based on personal data, and to keep such data sets intact and separate. And, of course, non-personal data are disconnected from any right on the behalf of the data subject.

Data, information (as such), irrespective of how private and how valuable it is, is not currently covered by property right.[34] No one owns personal data, although the 'data subject' in the EU holds some rights to it according to the GDPR.[35]

Notwithstanding this, if individual data fulfils the requirement for an intellectual property right, e.g. copyright, it can be covered by copyright (3rd party copyright, or copyright held by a firm that is also a gatekeeper to accessing the data in the server). Moreover, as discussed above, the firms providing the ecosystem or infrastructure of the IoT will have the infrastructure covered by patents and will also technically prevent access to the data. Traditionally, copyright owners regularly resort to technical protection measures (TPMs) (cf. Article 6 InfoSoc Directive), to prevent access to the copyright-protected content.[36] Interestingly, under the InfoSoc Directive not only is breaching these technical protection measures a copyright infringement, but also the manufacturing and sale of devices which have the primary purpose or effect of enabling such circumvention may be a copyright infringement in itself.[37]

---

[34] Zech is suggesting property right for non-personal data, Zech (2016), 51-79; there are authors who propose the recognition of ownership rights for consumers in the data they produce: Hoofnagle / Whittington (2014), 606-670.

[35] There are some rights connected to personal data in Articles 18-20 of the General Data Protection Regulation, such as the right to have data corrected, the 'right to be forgotten' and data portability. The latter right is limited, however, making it less attractive for consumers to change their social network. Cf. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1.

[36] See the interesting conference paper by Ciani (2018).

[37] Ibid.

Whether the data may be covered by rules regarding trade secrets has up until recently been regulated very differently in the different Member States.[38] However, the regulatory landscape for trade secrets is dramatically changing with the introduction of harmonized rules based on Directive 2016/943/EU of 8 June 2016 on the protection of trade secrets. It is probable that data may be protected under the rules in the directive. Individual data might not constitute a trade secret, but the combination of data or information (that as such is not publicly available), data sets, might well be covered.[39] The same argument also applies with regard to the requirement of commercial value under the directive.[40] Even if the publicly available data as such might not possess commercial value, their combination can acquire a certain value, conferring on the data holder a competitive advantage.[41]

Moreover, the interface between the rules of trade secrets and the right to data portability according to the GDPR is not fully sorted out.[42] While according to the old Data Protection Directive, data subjects could have an overriding right to transfer personal data, the data-portability right under the new Regulation is less clear on this point.[43] The reason for this shift could be that the GDPR aims to establish a high threshold for data protection and for the free movement of data, i.e. the fifth freedom of the internal market.[44] Possibly, in reference to this issue, the commercial reasons have been the overriding goal of data protection.

Database *sui generis* protection[45] may be applicable for holders of data. Government authorities (at least in the Nordic Member States) maintaining specific forms of data sets in databases, which they commercially provide access to (via the Internet), e.g. the national trade mark database or the databases for official addresses, land ownership, weather and maps etc., normally claim database protection as the basis for requiring re-users wishing to access the databases to enter into license agreements.[46] Private entities that collect customer or personal data in databases might, thus, also fulfil the requirements for obtaining data-base *sui generis* protection.

---

[38] Sweden is one of few Member States that have a specific act for the protection trade secrets, while, for example, trade secrets in the UK and in Denmark have been protected under case law and the marketing law (unfair competition law), respectively. In Sweden, collections of customer data, e.g. addresses, have been protected under the Trade Secret Act.

[39] See Drexl / Hilty / Desaunettes / Greiner / Kim / Richter / Surblytė / Wiedemann (2016), 6 et seq.

[40] Ibid.

[41] Ibid.

[42] Surblytė (2016), 14 et seq. Cf. Article 20(4) and Recital 63 GDPR.

[43] Ibid.

[44] The Swedish Trade Council (2016), 1 et seq.

[45] Directive No. 96/9/EC of the European Parliament and of the Council, of 11 March 1996 on the legal protection of databases, [1996] OJ L 77/20.

[46] See ECJ, Verlag Esterbauer, C-490/14, ECLI:EU:C:2015:735, in reference to maps, where the ECJ states that geographical data presented in maps can be deemed to be '*independent material*' within the meaning of Article 1(2) of the Database Directive, and it enjoys protection under the Database Directive.

From the general, brief, analysis above, even though possibly being a great source or wealth for the future, it is rather clear that data, be it big or open, personal or not, is not directly covered by any intellectual property legal system, while still heavily embedded in intellectual property rights protection and/or by neighboring legal protection. Indeed, the technical aspects of IoT are generally protected by patents, the investment in the collection of data may be protected by the *sui generis* data-base right and the data in aggregate may be a trade secret, though the data subject still holds some rights to it according to the GDPR (e.g. right to be forgotten and, possibly, data portability).[47]

Given the potential risk for 'thickets' it might also be concluded that neither data nor other technical, commercial or intellectual aspects of the developing data industry needs more intellectual-rights protection to flourish.[48] The protection is already on a high level. However, as hinted at above, if no one owns data there is no clear rule on whether the device producer, the network providers or algorithm providers or the cloud-service providers may exclude each other from the data. Who should trade with whom? This might cause competition policy problems. Competition could possibly be enhanced if the device producers could enter the data industry as independent stand-alone competitors. *Perhaps*, this requires that they should control ('own') the data created by their devices. Of course, this problem may be accentuated if there are network effects already present in the data industry giving the incumbent firms a head start.

4 Standards for the Internet of Things, Industrial Internet and IoT Patent Platforms or Pools

There is currently a global race for the IoT among standard-setting organizations (SSOs). Several different SSOs are fighting to become the SSO part of the collaborations that enact the standards for the new IoT era. Moreover, several pre-standard

[47] Cf. Art 18-20 GDPR. The rights to personal data should however be weighed against the other rights acknowledged by the Charter.

[48] In reference to the algorithms normally used to process data in databases. Drexl / Hilty / Desaunettes / Greiner / Kim / Richter / Surblytė / Wiedemann (2016), state: '[t]he Max Planck Institute for Innovation and Competition does not see any need to create special legal protection of algorithms used in data processing (e.g. in the context of big-data analysis)' and continue: 'concrete computer programs for processing data are already protected by copyright law of the Member States implementing Directive 2009/24/EC of 23 April 2009 on the legal protection of computer programs. Nevertheless, this protection covers neither the functionality of a computer program (judgment SAS Institute Inc., C-406/10, ECLI:EU:C:2012:259, paras 39-41) nor the underlying general algorithm (which is understood here as a set of rules to solve a problem step by step, independent of its expression and representation, e.g. the description of the steps to be made for analyzing or filtering data and the criteria to be applied). This is already implied by Recital 11 of the Directive, which clarifies that copyright protection for computer programs should not extend to the "ideas and principles which underlie any element of a program".' Some economists have suggested a property solution; cf. Hoofnagle / Whittington (2014), 606-670.

collaborations (consortia) are being formed including several different combinations of important players for the technologies that might be included in the IoT standards. These consortia are like pacts conducting lobbying and outright frontal attacks on other formations or pacts, all in the effort to get the 'right' technologies inside the relevant standards.

Of course, the incumbent SSOs are adapting to the new paradigm, e.g. ETSI, and even CEN and CENELEC, claim relevance in the IoT paradigm.[49] But there are special IoT SSOs. For example, in 2015 the Commission and various IoT players launched a large-scale alliance called AIOTI (Alliance for Internet Of Things Innovation) with the aim to assist the European Commission in the creation, establishment, designing of innovation and standardization policies.[50]

Whether these SSOs will be relevant in a world where Google (Brillo and Weave), Apple (HomeKit), Samsung (SmartThings), Amazon (Alexa) and Microsoft (Windows 10 IoT editions) are all bringing out their own IoT solutions is still to be seen. Perhaps there will be no market for the SSOs and one of these firms will instead become the *de facto* IoT standard just as Google's Android became the *de facto* open mobile OS?[51]

5 The Application of Competition Law

At least in reference to public data (so-called open data), competition law has been a great source of inspiration as a way to regulate the interaction between authorities and re-users. Cases like *Magill*,[52] *IMS Health*[53] and *Microsoft*[54] resemble and, presumably, influenced the way the Public Sector Information (PSI) Directive[55] has been drafted. Indeed, the interface between the PSI legislation and general competition law, especially the abuse-of-dominance doctrine in reference to (i) refusal to supply, (ii) exclusionary abuses and even (iii) discriminatory exclusion have been scrutinized by some national courts and competition authorities in conjunction with claims of breach of the PSI rules (the PSI Directive is discussed infra).[56]

However, the use of general competition-law doctrines such as refusal to supply (or the exceptional-circumstance doctrine) to gain access to datasets may be

[49] Cf. CEN and CENELEC (2016), 3 et seq.

[50] See Ciani (2018).

[51] Hughes (2016), 1 et seq.

[52] ECJ, RTE and ITP / Commission, C-241/91 and C-242/91, ECLI:EU:C:1995:98.

[53] ECJ, IMS Health, C-418/01, ECLI:EU:C:2004:257.

[54] GC, Microsoft / Commission, T-201/04, ECLI:EU:T:2007:289.

[55] The Directive on the re-use of public sector information (Directive 2003/98/EC, known as the 'PSI Directive') entered into force on 31 December 2003, [2003] OJ L 345/90. It was revised by Directive 2013/37/EU which entered into force on 17 July 2013, [2013] OJ L 175/1.

[56] Lundqvist (2013), 80 et seq.; Lundqvist / Vries / Linklater / Rajala Malmgren (2011), 11.

somewhat problematic.[57] Is the data holder dominant on a relevant market? With regard to e-platforms, Google and Facebook have been accused of holding market power due the popularity of their respective sites/ecosystems, but is that important in an upcoming IoT setting, where it will be the amount of and quality of data that creates market power? How should the relevant market be identified? Are there double or multisided markets,[58] and is such definition of the relevant market helping the competition-law analysis?[59] What about market power based only on the amount and importance of data, while the service to obtain the data is for zero price; could such a set up imply market power?[60] Moreover, in reference to the exceptional-circumstance doctrine: is accessing data an exceptional situation which requires the application of competition law? Perhaps the data can be duplicated with a reasonable effort. Indeed, data may be difficult to monopolize.[61] Furthermore, is there a second (downstream) market that the undertaking is reserving for itself? Is there an elimination of competition and the prevention of the appearance of a new product under the case law of *Magill*, *IMS Health* and *Microsoft*? Finally, is the data an indispensable input or even an essential facility under the same and similar lines of case law?

Indeed, in the scenario of a potential competitor wanting access to specific, unique datasets that are indispensable for conducting business, competition law has applicability, but that scenario is perhaps not so common. Moreover, can indispensability be considered identified when dealing with a dataset that by its specific size causes network effects to appear, to the point that the downstream or neighboring market is (or will be) monopolized?

This is a controversial issue depending on the definition of data. Social-interaction websites may tip the market to their favor due to network effects in the form of the

[57] In reference to PSBs, the issue has been whether they can be regarded as undertakings. Firstly, the data holder's activities with the data need needs to be analyzed in order to establish whether the holder in an undertaking in reference to Article 102 TFEU. Is the activity under scrutiny an economic activity, i.e. a commercial activity, conducted on a market? This may only be established if the end market, where the undertaking is facing its 'customers', is scrutinized. Of course, when dealing with private entities such as Google and Facebook etc., establishing whether they are undertakings or not may not cause a concern. However, when dealing with PSBs, it may cause problems. See the *Compass* case, where, according to the CJEU, an activity consisting in the maintenance and making available to the public of the data collected, whether by a simple search or by means of the supply of print-outs, in accordance with the applicable national legislation, did not constitute an economic activity, since the maintenance of a database containing such data and making that data available to the public are activities which cannot be separated from the public sector activity of collecting data. ECJ, Compass-Datenbank, C-138/11, ECLI:EU:C:2012:449, discussed in Lundqvist (2013), 80 et seq.

[58] Evans / Noel (2008), 663-695 and Filistrucchi / Geradin / v. Damme / Affeldt (2014), 293- 339.

[59] Ibid. Evans / Noel (2008) and Filistrucchi / Geradin / v. Damme / Affeldt (2014) agree that not all digital markets are multisided. For an interesting analysis that e-platforms are not multisided markets see Newman (2013), 3 et seq.

[60] See Bundeskartellamt (2016). OECD (2016). Autorité de la Concurrence and Bundeskartellamt (2016), 7, 14 et seq.

[61] Sokol / Comerford (2017).

number of social connections (i.e. connected friends). But are the 'friends' or 'connections' interconnected on a social website data, and is it data that can be transferred? Possibly, Article 20 of the GDPR does grant users that right to portability of such data and even personal data generated by the data subject's activity.[62] Thus, it seems that data subjects may transfer data, making the data subject a market player.

But what about competition law? Can access to data be granted under the exceptional-circumstance doctrine? Notwithstanding the above, the *Magill*[63] 'logic' works well in a data scenario: entities (in the *Magill* case the publicly owned BBC and RTE *et al.*), engaging in their primary market or (public) task (producing and distributing TV programs), create or collect information, (in the form of TV listings) that might be copyright-protected. They are, under the rules of abuse of dominance, required to give access to this information (the TV listings), due to its indispensability and because a refusal would be unjust, to an undertaking that will create a new product (TV guides). Thus, in the *Magill* case the appellants were not allowed to reserve for themselves a secondary market. In an IoT setting the device producers would collect (create) information from the devices included in the product sold to the consumers. Likewise, the e-platform providers collect data as a by-product for the service provided.

The *Magill* case dealt with unique data in the sense that the TV listings could not be obtained from any other source. Also, *IMS Health* dealt with a unique brick structure (a *de facto* standard for the industry) developed by IMS and the users in conjunction. *Magill* may be used to argue access to certain specific kinds of datasets under the exceptional-circumstance doctrine, while general data, user-generated data and data voluntarily provided by users will, however, especially after the introduction of IoT, perhaps not be indispensable, thus not causing the doctrine to be triggered.[64] Indeed, in the future certain devices, e.g. cars, refrigerators, mobile phones etc., might be able to collect the same or similar personal data from us as we today provide Facebook and Google. Moreover, the data that can potentially be collected by these devices may have a high quality, and may be more efficient and effective in trying to map the general consumer, than the information that consumers of social sites on the Internet are currently voluntarily providing.

The issue of whether general competition law (more specifically the exceptional-circumstance doctrine) will be applicable to access general personal data, i.e. the personal information that people are generating by utilizing the internet, has not yet

[62] Article 29 Working Party (2016), p. 9: '[f]or example, a webmail service may allow the creation of a directory of a data subject's contacts, friends, relatives, family and broader environment. Since these data are relating to, and are created by the identifiable individual that wishes to exercise his right to data portability, data controllers should transmit the entire directory of incoming and outgoing e-mails to the data subject'.

[63] ECJ, RTE and ITP/Commission, C-241/91 and C-242/91, ECLI:EU:C:1995:98.

[64] An argument frequently posed by the opponents of applying the essential-facilities doctrine is that data cannot be easily monopolized: it is non-rival and, they argue, non-exclusive, since there are no contracts preventing users from sharing their personal information with multiple companies. Furthermore, they argue that there are few entry barriers to new platforms, as data is relatively inexpensive to collect, short-lived and abundant. Balto / Lane (2016), 4 et seq.

been conclusively scrutinized by any competition law court. Nonetheless, it can be questioned whether a court would find the exceptional-circumstance doctrine applicable. The doctrine may in a few cases be applicable, it depends on the data set collected. It will also depend on the actual size and magnitude of the data collected. As discussed above, there might be network effects involved in the data industry, which may be a reason to make the exceptional-circumstance doctrine applicable. If the data collected is so vast that it creates a tipping effect making it impossible to rebuilt a similar data set, the exceptional-circumstance doctrine may, possibly, become applicable. Moreover, the antitrust harm of discriminatory exclusion should be taken into consideration. Could Google and Facebook be accused of discriminatory refusal to sell data to a competitor when using their data to sell adds to third parties?

There are a few competition-law cases dealing with big data originating from activities and decisions by EU Member States' competition authorities. There are a few French cases, e.g. *GDF*[65] and *EDF*,[66] concerning discriminatory re-use of datasets, where the data sets seem not to have been considered essential or indispensable for entering the relevant market, but where the data holder used the data sets in an exclusionary fashion. Access was not granted on fair terms vis-à-vis potential competitors in a downstream market or in neighboring businesses.[67]

A third French case, *Cegedim*, dealt with medical data used by pharmaceutical companies to manage their visits to doctors and pharmacies in France. Cegedim was accused of refusal to sell, on a discriminatory basis, datasets regarding medical information.[68] Cegedim was a leader in the medical database market, in which it has a dominant position, offering both databases and customer-management software to laboratories. It notably produces the OneKey database, the most widely used database in the industry. Euris, a company that only produces customer-management software but no databases, accused Cegedim of abusing its dominant position, as Cegedim refused to sell its OneKey database to laboratories that were using the

[65] The *Autorité de la Concurrence*, France's competition authority, imposed an interim measure on GDF, ordering that gas supplier to grant its competitors access to some of the data it collected as a provider of regulated offers, in particular consumption data. The aim of this interim measure was to allow all suppliers to have the same level of relevant information to make offers to consumers (no public information or private database exists on households subscribing to gas contracts). French Competition Authority, Decision 14-MC-02 of 09.09.2014. Due to privacy laws, the transmission of GDF data to competitors was conditional to an approval by consumers. A significant share of the consumers did refuse that their data be transferred from GDF to competing operators. The case is discussed in the joint report by the Autorité de la Concurrence and Bundeskartellamt (2016), 20.

[66] French Competition Authority, Decision n°13-D-20 of 17.12.2013, confirmed on that points by the court of appeal on 21.05.2015.

[67] A similar reasoning has also been used in some merger cases. For instance, in its EDF/Dalkia merger decision: European Commission, Case No. COMP/M. 7137 - EDF/Dalkia en France, 25 June 2014.

[68] French Competition Authority, Decision n° 14-D-06, dated 08.07.2014, relative à des pratiques mises en œuvre par la société Cegedim dans le secteur des bases de données d'informations médicales. This decision has been confirmed on appeal but is still pending in front of the Cour de Cassation (the French Supreme Court).

software marketed by Euris, whereas it agreed to sell OneKey to laboratories using software developed by other competitors. In accordance with the Autorité's precedents, as well as European Court of Justice case law, the Autorité de la Concurrence found that access to the OneKey database was not indispensable to Cegedim's competitors on the downstream market for customer-management softwares, and thus the OneKey database was not an essential facility.[69]

However, the Autorité de la Concurrence established that Cegedim maintained a continuous and unilateral refusal to grant access to OneKey specifically targeting actual or potential clients of Euris. This difference in treatment of companies in otherwise similar situations constituted, in the Autorité's view, a form of discrimination for which Cegedim was unable to provide any objective justification. As a result, this practice had a seriously harmful effect on Euris (which lost 70% of its customers between 2008 and 2012) and restricted the laboratories in their choice of customer-management software. Hence the Autorité de la Concurrence concluded that Cegedim had abused its dominant position through exclusionary discrimination.[70]

Similarly, the Belgian competition authority adopted in 2015 a settlement decision finding that the national lottery body was abusing its dominant position. The lottery was found to have been using its client database, created under its legal monopoly for public lotteries, when selling its new sports-betting products, in a market where they faced competition, while refusing access to competitors. Indeed, the Belgian lottery body was re-using unique data sets on competitive markets.[71] Possibly these cases show a new form of antitrust harm (or 'new non-discrimination theory') whereby a dominant firm cannot 'self-preference' its 'own operations over those of competitors' in a discriminatory way. Indeed, they give some room for the EU Commission to find a similar antitrust harm in the ongoing Google investigation.[72]

There are also a few Nordic competition authority cases. In *Swedish Patent and Registration Office* (PRV)[73] from March 2012, PRV began to offer free access to the trademark register database to the downstream end-user market, whereas customers on the upstream wholesale market were offered more detailed data in different formats (so-called register-lifted data) for a one-time fee and then a yearly fee. PRV was accused of marginal squeeze by selling access to the data in wholesale market while giving access for free to consumers on its own website. PRV, acknowledged as being an 'undertaking', was considered dominant in the market of providing access to the specific trademark database according to the SCA, while PRV disputed the charges of marginal squeeze and price discrimination. In the end, PRV lowered its fees to marginal cost, and the case was settled.

[69] ECN Brief (2014).

[70] Ibid.

[71] Platteau (2015), 1 et seq.

[72] Petit (2015), 1 et seq. and Vesterdorf (2015), 4.

[73] SCA, *The Swedish Patent and Registration Office*, Dnr 470/2011, from September 2012.

In *The Land Registry*, from November 2012, the SCA assessed the way the cadaster sold refined information in the land register to commercial private actors. The complaining re-user purported that the cadaster was abusing its dominant position by not giving access to raw data. Instead, the re-user only got access to more refined data. The SCA did not, based on the facts of the case, find any abuse.[74]

The above scarce cases show that there is room for competition law in the context of big data, though access to raw datasets might be difficult under competition law. When the data set is indispensable access might be granted, and there are cases concerning discriminatory exclusion which might create a duty to deal. Competition law will still have an important role to play with respect to big data, with possible abuses, such as marginal squeeze (see PSI-related cases), discriminatory access to personal data, though this is not essential data (see French cases and also PSI-related cases), exclusivity arrangements (The EU Commission Google investigation and collaborations in reference to the cultural sector under the PSI Directive), violation of data-protection rules when obtaining personal data, exploitative abuse (German Facebook case[75]), and perfect monopoly pricing (eCall), and, moreover, excessive collection of personal data might be considered an excessive abuse if the notion of users as 'paying' with personal data when using 'free' services on the Internet is correct.[76]

Moreover, competition law will still be a useful tool to regulate SEPs when the standards of the IoT materialize. It is easy to predict that in the future, when the brick-and-mortar industries start producing interconnected 'things', the notion of patent war may take a whole new meaning. Indeed, the *Huawei* case and the issues it has raised may very well be addressed again by the EU Courts.

6 Sector-Specific Regulations and Data-Protection Rules

Sector-specific regulations seem to be the tool to use to access competitors' data in the twenty-first century.

There seems to be a need for rules regarding fair access to data. The PSI Directive mentioned above stipulates routes for accessing government data. The main focus

[74] SCA, *The Swedish Land Registry*, Dnr. 601/2011, from November 2012.

[75] Bundeskartellamt, Press release: Bundeskartellamt initiates proceeding against Facebook on suspicion of having abused its market power by infringing data protection rules, 2 March 2016. See also for instance, in Allianz Hungária, the ECJ held that the impairment of objectives pursued by another set of national rules could be taken into account to assess whether there was a restriction of competition (in this instance, by object). Referring to German Competition law, the German Federal Court of Justice has stated that contract terms which are incompatible with the laws regulating general conditions and terms of trade might be an abuse of a dominant position if the use of the terms is based on the company's market dominance". ECJ, Allianz Hungária Biztosító and others, C-32/11, ECLI:EU:C:2013:160. See also German Federal Court of Justice (Bundesgerichtshof), VBL-Gegenwert, KZR 61/11 16 November 2013, para. 68.

[76] Kerber (2016).

of the PSI Directive is very specific. It is to create a level playing field when making available PSI as input to a commercial activity, i.e. when the PSI is used as components to new products and services. This should then release the full economic potential of a new emerging area of the ICT sector.[77] If PSBs offer information products or services exclusively, chances are that they will not be able to provide these services as innovatively and efficiently as a structure governed by competition would be able to.[78] This could have a negative effect on competition in the European market. Therefore, the PSI Directive aims to overcome these barriers, which limit the re-use of PSI in EU Member States. The PSI Directive thereby stipulates that public-sector data collectors should grant access to data. The public-sector data collector is even obliged to grant access if it re-uses data collected commercially by selling access to the database to data brokers or re-users. The PSI Directive tries to negate barriers which could include attempts by PSBs to charge supra-competitive prices, unfair competition between the public and the private sector, practical issues hindering re-use (like the lack of information on available PSI), and the attitude of PSBs failing to realize the economic potential of PSI.[79] The PSI Directive is triggered by three sets of questions:

1. Is the data created (supplied) outside or inside the public task of the PSB? If so, what is the initial purpose for producing the data? Is it to fulfill a public task? If yes, the second question is:
2. Are the documents being re-used by the PSB or some other body on its behalf? In other words, will the data be used for another purpose than the initial purpose? Moreover, will this re-use constitute a commercial activity, e.g. giving access to the dataset to paying subscribers?
3. If so, then a number of requirements will apply, including that third parties have the right to access the dataset on something similar to FRAND terms, so as to enable the third parties to commercially utilize the open data in competition with the PSB and other firms that have access to the dataset.

Interestingly, the PSI Directive seems to include a non-discriminatory exclusion rule similar to the ideas put forward in the French cases *GDF*[80] and *EDF*[81] discussed above.

The very interesting eCall Regulation[82] should also be mentioned. According to Recital 16,

---

[77] EU Commission (1998), 5.

[78] Lundqvist (2011), 17.

[79] Janssen / Dumortier (2011), 195-195.

[80] French Competition Authority, Decision 14-MC-02 of 09.09.2014. The case is discussed in the joint report by the Autorité de la Concurrence and Bundeskartellamt (2016), 20.

[81] French Competition Authority, Decision n°13-D-20 of 17.12.2013, confirmed on that points by the Court of appeal on 21.05.2015.

[82] Regulation (EU) 2015/758 of the European Parliament and of the Council of 29 April 2015 concerning type-approval requirements for the deployment of the eCall in-vehicle system based on the 112 service and amending Directive 2007/46/EC, [2015] L 123/77.

> [i]n order to ensure open choice for customers and fair competition, as well as encourage innovation and boost the competitiveness of the Union's information technology industry on the global market, the eCall in-vehicle systems should be based on an interoperable, **standardised, secure and open-access platform** for possible future in-vehicle applications or services. As this requires technical and legal back-up, the Commission should assess without delay, on the basis of consultations with all stakeholders involved, including vehicle manufacturers and independent operators, all options for promoting and ensuring such an open-access platform and, if appropriate, put forward a legislative initiative to that effect. Furthermore, the 112-based eCall in-vehicle system should be accessible **for a reasonable fee** not exceeding a nominal amount and without discrimination to all **independent operators for repair and maintenance** purposes in accordance with … [emphasis added].[83]

The *eCall* regulation seems to lay the groundwork for a future in which competitors will be able to access data originating from cars used by individuals. Specifically, this groundwork is that the device should be, or be connected to, a standardized, secure and open-access platform. Interestingly, the idea seems to be that by creating a standard, competitors will be enabled not (only) to produce eCall machines under FRAND licenses, but to actually access eCall machines in the cars with their own applications in order to pick up data. It is thus envisioned that the automobile manufacturers should not have an exclusive right to the personal data created in the car (or the device), but should perhaps open up the platform in the car to, for example, leasing firms, insurance companies and independent service providers, who will be able to access the device in order to collect data.[84]

Finally, the recently updated Payment Services Directive (PSD) stipulates a right for third parties under certain circumstances to access the banking data of consumers. Consumers should be able to agree to third parties providing services by accessing consumer bank accounts and Internet bank sites. PSD II may, to promote competition, require banks to provide standardized API access to third parties under the auspices of the European Banking Authority (EBA).[85] This may enable third parties to use data collected by a competitor to tailor their banking service to customers.

These three Directives are examples of rules that are, or are close to, requiring competitors to give access to data, or to devices and platforms, so as to enable data harvesting. It may be an indication of an interesting underlying current that the

---

[83] Ibid.

[84] An example of this development could be the '5G Automotive Association', announced on 27 September 2016 by AUDI AG, BMW Group, Daimler AG, Ericsson, Huawei, Intel, Nokia and Qualcomm Incorporated. The association will develop, test and promote communications solutions, support standardization and accelerate commercial availability and global market penetration. The goal is to address society's connected mobility and road-safety needs with applications such as connected automated driving, ubiquitous access to services and integration in smart cities and intelligent transportation; available at: https://www.ericsson.com/en/news/2016/9/telecommunications-and-automotive-players-form-global-cross-industry-5g-automotive-association-.

[85] See Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, [2015] OJ 337/35. Cf. Commission (2015).

legislature is trying to boost competition by granting access to competitors' data while circumventing general competition law. The idea is to boost competition, without making use of any test of antitrust harm, by opening up the device to everyone for collecting data. Whether such a policy is pro-competitive may be disputed. Not only new entrants will be able to obtain data; also incumbent e-platform firms will try to access these devices or, with respect to government data, the PSI. This may act as a deterrent for brick-and-mortar firms to become full-fledged competitors in the data industry. Indeed, the incentive to become members of the data industry may be low if a brick-and-mortar firm knows that it is obliged to share the input data, i.e. its raw material. Moreover, it also begs the question, to be put to the legislature, why similar access rules do not exist in other industries. Why should they not apply to e-platform providers when large industries such as the car industry and the bank sector are required to give access?

Data-protection rules, whether they should be used as a benchmark for finding competition law violations,[86] or whether they should be considered, and altered to, something of an (intellectual) property right (that competition law can 'trump'), is an issue up for grabs to be solved by researchers and practitioners in the twenty-first century. Possibly, data-protection rules and the interface between data protection rules and competition law may become topics for sector-specific regulations in the future.

When re-users or data brokers are interviewed, they express the sentiment that data-protection rules are the grand 'show stopper', and the issue for these firms is whether competition law can be used to override data-protection rules. Can competition law trump data-protection rules? From the case law of the European Commission, it seems difficult. In *Asnef-Equifax* the CJEU stated that 'any possible issues relating to the sensitivity of personal data are not, as such, a matter for competition law [and] may be resolved on the basis of the relevant provisions governing data protection.'[87] Moreover, in the *Facebook/WhatsApp*[88] merger case, the Commission states that '[a]ny privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules'. Finally, the argument put forward against using competition law to trump data-protection rules is that reduction in privacy equals reduction in quality, and that is not the same thing as using competition law to trump an intellectual property right. 'Quality' may be an objective of competition law itself, while upholding property rights is less so.

The European Data Protection Supervisor has, in 2014, indicated a shift in policy, with a 'more holistic approach to enforcement', in which a more systematic dialogue is to be maintained between competition, consumer and data protection authorities. However, the collaboration between DG Connect and DG Competition seems rather unlikely.

---

[86] Bundeskartellamt (2016).

[87] ECJ, Asnef-Equifax, C-238/05, ECLI:EU:C:2006:734, para. 63.

[88] European Commission, Case No. COMP/M.7217,Facebook/WhatsApp, 3 October 2014, para. 164.

7 Conclusion

Competition law clearly still has a place and use in the big data industry.[89] However, when defining the role for competition law certain aspects should be taken into consideration: (i) the sources of data are increasing in number and possibly also in quality; (ii) access seems to be granted by sector-specific regulation, rather than through general competition law. Nonetheless, competition law still has an important role to play with regard to big data, with possible abuses, such as, for example, marginal squeeze (PSI-related cases), discriminatory access to personal data, though not being essential data (French cases, PSI-related cases and possible European Commission investigation into Google's search-bias conduct), exclusivity arrangements (Google investigation), violation of data protection rules when obtaining personal data, exploitative abuse (German Facebook case) and perfect monopoly pricing (eCall), and even excessive collection of data might be an antitrust harm in itself. In fact, perfect monopoly discrimination can possibly be achieved by utilizing data on certain markets. Moreover, (tacit) collusion may be facilitated through utilizing data and algorithms.[90]

Notwithstanding the above, the IoT also raises competition-policy issues. To create a competitive market for data in the upcoming IoT society, the brick-and-mortar firms need to enter the data industry and become stand-alone collectors and sellers and licensors of datasets. Brick-and-mortar firms entering the data industry would benefit competition and create wealth for the consumers to harvest. However, the current trend from the legislature seems not to benefit this development, and, in fact, current legislative efforts rather facilitate a scenario in which other firms, including incumbent data-industry firms, gain access to data collected by their potential competitors in the brick-and-mortar industry. As discussed in this paper, sector-specific regulation of large industries such as the car industry and the bank sector with reference to public data requires or may soon require firms to give access to data or the devices collecting data to any comer without requiring an analysis of antitrust harm.

The data collected by the devices of the brick-and-mortar industry should instead possibly belong to the respective device producers; and they should be encouraged to develop their own cloud services and algorithms, and should not be forced (or encouraged) to enter into collaborations with third parties, e.g. network providers or incumbent e-platform firms, to *de facto* transfer the valuable data.

References

Balto, D. / Lane, M. (2016), Monopolizing Water in a Tsunami: Finding Sensible Antitrust Rules for Big Data, available at: http://ssrn.com/abstract=2753249

[89] Not alone of this opinion: Grunes / Stucke (2015), 2 et seq.

[90] Ezrachi / Stucke (2016).

Chisholm, A. / Jung, N. (2015), Platform Regulation— Ex-Ante versus Ex-Post intervention: evolving our antitrust tools and practices to meet the challenges of a digital economy. Competition Policy International. Vol. 11, No. 1, 7-21

Ciani, J. (2018), A Competition-Law-Oriented Look at the Application of Data Protection and IP Law to the Internet of Things: Towards a Wider 'holistic approach', in this volume

De Mauro, A. / Greco, M. / Grimaldi, M. (2016), A Formal Definition of Big Data Based on its Essential Features, Library Review, Vol. 65, No. 3, 122-135, available at: http://www.emeraldinsight.com/doi/pdfplus/10.1108/LR-06-2015-0061

Drexl, J. / Hilty, R. / Desaunettes, L. / Greiner, F. / Kim, D. / Richter, H. / Surblytė, G. / Wiedemann, K. (2016), Data Ownership and Access to Data Position Statement of the Max Planck Institute for Innovation and Competition, Max Planck Institute for Innovation and Competition Research Paper No. 16-10, 6, available at: http://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/positionspaper-data-eng-2016_08_16-def.pdf

Drexl, J. (2015), The Competition Dimension of the European Regulation of Public Sector Information and the Concept of an Undertaking, in: J. Drexl / V. Bagnoli (Eds.), State-Initiated Restraints of Competition (ASCOLA competition law), 64-100, Edward Elgar

Evans, D. / Noel, M. (2008), The Analysis of Mergers that Involve Multisided Platform Businesses, Journal of Competition Law & Economics 4(3), 663-695

Filistrucchi, L. / Geradin, D. / v. Damme, E. / Affeldt, P. (2014), Market Definition in Two-Sided Markets: Theory and Practice, Journal of Competition, Law & Economics, Vol. 10, No. 2, 293-339

Ezrachi, A. / Stucke, M. (2016), Virtual Competition The Promise and Perils of the Algorithm-Driven Economy, Harvard University Press

Grunes, A. / Stucke, M. (2015), No Mistake About It: The Important Role of Antitrust in the Era of Big Data Antitrust Source Online; University of Tennessee Legal Studies Research Paper No. 269, available at: http://ssrn.com/abstract=2600051

Hoofnagle, C.J. / Whittington, J. (2014), Free: Accounting for the Costs of the Internet's Most Popular Price, UCLA Law Review, Vol. 61, 606-670

Janssen, K. / Dumortier, J. (2011), Towards a European Framework for the Re-use of Public Sector Information: a Long and Winding Road, International Journal of Law and Information Technology 2, 195-195

Kerber, W. (2016), Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection with references, MAGKS, Joint Discussion Paper Series in Economics, No. 14-2016, available at: http://ssrn.com/abstract=2770479 or https://doi.org/10.2139/ssrn.2770479

Lexinnova (2014), Internet of Things: Patent Landscape Analysis, LexInnova Technologies, LLC

Lundqvist, B. / de Vries, M. / , Linklater, E. / Rajala Malmgren, L. (2011), Business Activity and Exclusive Right in the Swedish PSI Act, Report, Swedish Competition Authority, available at: http://www.konkurrensverket.se/globalassets/english/publications-and-decisions/business-activity-and-exclusive-right-in-the-swedish-psi-act.pdf

Lundqvist, B. (2013), Turning Government Data into Gold: The Interface Between EU Competition Law and the Public Sector Information Directive - With Some Comments on the Compass Case, International Review of Intellectual Property and Competition Law, Vol. 44, Nr. 1, 79-95

Newman, N. (2013), Search, Antitrust and the Economics of the Control of User Data with references, Yale Journal on Regulation, Vol. 30, No. 3, 2014, available at SSRN: http://ssrn.com/abstract=2309547 or https://doi.org/10.2139/ssrn.2309547

Petit, N. (2015), Theories of Self-Preferencing Under Article 102 TFEU: A Reply to Bo Vesterdorf, available at: https://ssrn.com/abstract=2592253 or https://doi.org/10.2139/ssrn.2592253

Platteau, K. (2015), National Lottery settles abuse of dominance case with Competition Authority, available at: http://www.internationallawoffice.com/Newsletters/Competition-Antitrust/Belgium/Simmons-Simmons/National-Lottery-settles-abuse-of-dominance-case-with-Competition-Authority

Shapiro, C. (2001), Navigating the Patent Thicket: Cross Licenses, Patent Pools and Standard Setting, in: A. Jaffe, J. Lerner, S. Stern (Eds.), Innovation Policy and the Economy (MIT Press), 119

Surblytė, G. (2016), Data Mobility at the Intersection of Data, Trade Secret Protection and the Mobility of Employees in the Digital Economy, 14 et seq., Max Planck Institute for Innovation & Competition Research Paper No. 16-03, available at: http://ssrn.com/abstract=2752989 or https://doi.org/10.2139/ssrn.2752989

Sokol, D. / Comerford, R. (2017), Does Antitrust Have a Role to Play in Regulating Big Data?, in: R. Blair and D. Sokol (Eds.), Cambridge Handbook of Antitrust, Intellectual Property and High Tech (Cambridge University Press), available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2723693

Stucke, M. / Grunes, A. (2016), Big Data and Competition Policy, Oxford University Press

Vesterdorf, B. (2015), Theories of Self-Preferencing and Duty to Deal – Two Sides of the Same Coin, 1(1) Competition Law & Policy Debate, 4

Zech, H. (2016), Information as a tradable commodity, in: A. De Franceschi (Ed.), European Contract Law and the Digital Single Market (Intercentia), 51-79

Additional Sources

Autorité de la Concurrence and Bundeskartellamt (2016), Competition Law and Data, available at: http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf

Bundeskartellamt (2016), Press release: Bundeskartellamt initiates proceeding against Facebook on suspicion of having abused its market power by infringing data protection rules, 2 March 2016, available at: http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html?nn=3591568

CEN and CENELEC (2016), position paper on standard essential patents and fair, reasonable and non-discriminatory (FRAND) commitments, available at: http://www.cencenelec.eu/News/Policy_Opinions/PolicyOpinions/EssentialPatents.pdf

Commission Statement of Objections to Google on Android operating system and applications, European Commission, Press release (IP/16/1492), Antitrust: Commission sends Statement of Objections to Google on Android operating system and applications, 20 April 2016, available at: http://europa.eu/rapid/press-release_IP-16-1492_en.htm

ECN, ECN Brief 04/2014 (2014), available at: http://ec.europa.eu/competition/ecn/brief/04_2014/brief_04_2014.pdf

EU Commission (1998), Public Sector Information: A Key Resource for Europe, Green Paper on Public Sector Information in the Information Society, COM(1998) 585 final, 5

EU Commission (2015), A Digital Single Market Strategy for Europe, COM(2015) 192 final, available at: https://ec.europa.eu/digital-single-market/en/news/digital-single-market-strategy-europe-com2015-192-final

EU Commission (2016), Press Release, Statement of Objections to Google on Android operating system and applications, 20 April 2016, available at: http://europa.eu/rapid/press-release_IP-16-1492_en.htm

French Senate Report (2013), available at: http://www.senat.fr/rap/r12-443/r12-443.html

OECD (2015), Data-Driven Innovation - Big Data for Growth and Well-Being, available at: http://www.oecd.org/sti/ieconomy/data-driven-innovation.htm

Hughes, T. (2016), A world with more IoT standards bodies than IoT standard, available at: http://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/A-world-with-more-IoT-standards-bodies-than-IoT-standards

OECD (2016), Big Data – Bringing Competition Policy to the Digital Era, available at: http://www.oecd.org/daf/competition/big-data-bringing-competition-policy-to-the-digital-era.htm

Östman, N. (2016), The IP of Things, LinkedIn available at: https://www.linkedin.com/pulse/ip-things-niklas-%C3%B6stman?trk=prof-post

The Swedish Trade Council (2016), Data flows – a fifth freedom for the internal market? Report, available at: https://www.kommers.se/Documents/dokumentarkiv/publikationer/2016/Data%20flows%20-%20A%20fifth%20freedom%20for%20the%20internal%20market.pdf

Working Party under Article 29 of Directive 95/46/EC (2016), Guidelines on the right to data portability in the GDPR, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp114_en.pdf

A Competition-Law-Oriented Look at the Application of Data Protection and IP Law to the Internet of Things: Towards a Wider 'Holistic Approach'

Jacopo Ciani

Contents

1 What Is the Internet of Things? 216
1.1 Uses and Application in Contexts 217
1.2 Industry Impact and Future Trends 219
2 The Role of Law in the IoT 219
2.1 Threat to Privacy: Passive Data Transmission 220
2.2 Property Interest in 'Big Data' and Market Power Based on Data Ownership: The Intersection of Big Data and Antitrust Law 223
3 Protecting and Enforcing IoT Technologies Through Intellectual Property Rights 226
3.1 Patents 227
3.2 Software 228
3.3 Trade Secrets 230
3.4 Database Protection 231
3.5 Technical Protection Measures 231
4 The Value of and the Obstacles to Interoperability 233
4.1 Legal Tools to Safeguard Interoperability 234
4.2 Obstacles to Effective Interoperability 236
4.3 Interoperability in the IoT: Competition-Law Issues in the Standardisation Context 237
5 Personal Data, Competition and IP Law: Towards a 'Holistic Approach'? 239
6 The Policy Framework for Regulating Standard-Setting in the EU 241
7 Conclusion 243
References 243

Abstract Business models in the digital economy increasingly rely on wireless communications capabilities, which make it possible to receive, collect and send a myriad of user data. As the intensity and magnitude of this technological revolution, widely known as the 'Internet of Things' (IoT), are mostly unknown to date, the law

Jacopo Ciani is PhD at University of Milan, research fellow at University of Turin and lawyer at Tavella Studio di Avvocati in Milan.

J. Ciani (✉)
University of Turin, Turin, Italy
e-mail: jacopo.cianisciolla@unito.it

M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law*, MPI Studies on Intellectual Property and Competition Law 28, https://doi.org/10.1007/978-3-662-57646-5_9

may struggle to evolve quickly enough to address the challenges it poses. Many of the legal issues arising from smart devices relate to user privacy and device security. Moreover, it is worth considering how the ownership of data that flow through the IoT and their impact on market power may potentially lead to anti-competitive concerns by creating or reinforcing a dominant market position. After noting the state of the law with regard to these areas, this chapter will focus on the impact of IP rights covering IoT technologies on lock-in strategies aimed at foreclosing interoperability with competitors' technologies. It will discuss when IP rights could lead to anticompetitive concerns by creating or strengthening a dominant market position and whether the actual set of laws has the antibodies needed to discourage these unfair competition practices. It will be suggested that these issues should be explored at the intersection of data protection, intellectual property, competition law and standard-setting public policy. In this regard, the European Data Protection Supervisor's 'holistic approach', initiated to bring privacy concerns into merger investigations, might have a significantly wider horizon in the IoT context and open up a closer dialogue between regulators.

1 What Is the Internet of Things?

The first use of the term 'Internet of Things' has been attributed to Kevin Ashton, who used it in the title of a 1998 presentation with the meaning of 'things using data they gathered without any help from us'.[1] The IoT refers to a collection of everyday physical 'smart devices' equipped with microchips, sensors and wireless communications capabilities and connected to the Internet and to each other, which can receive, collect and send a myriad of user data, track activities and interact with other devices in order to provide more efficient services tailored to users' needs and desires.[2]

Therefore, IoT technology basically consists of three core elements: (1) devices (physical components), (2) protocols for facilitating communication between smart devices (connectivity components) and (3) systems and methods for storing and analysing data acquired by the smart devices ('smart' components).[3] By embedding

[1] Ashton (2009). During the presentation he stated that adding radio-frequency identification devices (RFID chips) to everyday objects will create an Internet of Things. For a brief history of the IoT see Ferguson (2016), 813.

[2] The FTC (2015), 1, defines IoT as 'an interconnected environment where all manner of objects have a digital presence and the ability to communicate with other objects and people'.

[3] To be more precise, the IoT system architecture needs: appropriate sensors imbedded in all objects that can allow them to give their location and status; wireless connection to the Internet; appropriate mediating software between the object, the Internet and other objects; operator interfaces; encryption algorithms for security; operating platforms and protocols to manage the vast amount of competing data being exchanged. See Porter / Heppelmann (2014).

sensors and actuators[4] these objects, that are networked through an open Internet protocol, will no longer be simply physical objects but rather intuitive, sensing, automated and communicating information technologies.[5] In simple terms, the IoT is the idea of everyday objects informing and being informed about other objects, via connection over the Internet.

1.1 Uses and Application in Contexts

Predictions say that a truly 'programmable world' will exist.[6] There is no shortage of examples of things the IoT could do. Intelligent vehicles able to monitor their speed according to the limits, the pollution index or the fuel price could be just a first example of a computing device everybody owns.[7] Similarly, smartphones may gather worlds of information: heartbeats per minute, driving logistics, sleep habits and much more. Smart fridges will be able to understand what has run out and even take care of the shopping by 'calling' the local supermarket to order food. Wellness trackers with diagnostic capabilities can identify medical problems, engage patients in healthier behaviour and reduce medical intervention, with significant cost savings.[8] Other examples include smart thermostats, home-security web-cams, smart

[4] Most of the automation in IoT is carried out through the combined use of sensors and actuators, which form the backbone of IoT. Sensors are used for collecting data, which may be processed, analysed, reported or used to trigger another event or other devices into operation.

Consider a situation in which you would like your heating to be switched on when the house temperature goes below a certain level. This system would work with a sensor to measure the temperature. Once the sensor determines that the temperature has gone below the set level, it sends an alert to the controller. The controller uses inputs and outputs in the same way an ordinary computer does. Inputs capture information from the user or the environment, while outputs do something with the information that has been captured. In the above example, the controller would trigger an actuator, which is a device that converts energy into a mechanical action; in this case, switching on the heating.

[5] Rose (2014) defines them as 'enchanted objects'; Kominers (2012), 3, speaks of 'intelligent objects'.

[6] Alex Hawkinson, CEO and founder of SmartThings, referred to a 'programmable world' where 'things will become intuitive [and] connectivity will extend even further, to the items we hold most dear, to those things that service the everyday needs of the members of the household, and beyond'. Cf. What Happens When the World Wakes up, Medium (23 September 2014), available at: https://medium.com/@ahawkinson/whathappens-when-the-world-wakes-up-c73a5c931c17.

[7] A pay-as-you-drive (PAYD) insurance monitoring device can provide a detailed look into the use of the vehicle (location, time, distance, speed and other parameters) and influence an insurance premium. For an overview of possible uses connected to cars see Cunningham (2014), 138.

[8] Remote patient monitoring (RPM), also called homecare telehealth, is a type of ambulatory healthcare that allows a patient to use a mobile medical device to perform a routine test and send the test data to a healthcare professional in real time. See Terry (2016), 347, exploring these emerging Internet of Health Things (IoHT) technologies, which are going to disrupt conventional models of healthcare.

coffee machines, fitness trackers, watches, cars, light bulbs, washers and dryers, toasters, toothbrushes, smart meters[9] and many other things.[10]

Given that the Internet might potentially become part of any object around us, it is not surprising that some scholars prefer to speak of the 'Internet of Everything'.[11] Indeed, as the cost of microchips, sensors, cameras, circuits and software continues to fall,[12] these technologies are increasingly embedded in almost all devices that consumers own and encounter.

Commentators have suggested that what makes IoT fundamentally different is not the Internet, but the changing nature of 'things'. It is the new set of product functions and capabilities that is reshaping industry structure and altering the nature of competition.[13]

For consumers, who may control and interact with these devices through apps on their smartphones, IoT technologies will provide new services that will make their lives and jobs easier. That is especially the case of the subset of IoT technologies known as 'wearables'.

On a larger scale, the IoT can include industrial controls (even on employees' behaviour and performance[14]) and factory machinery. For firms, the IoT has great potential to create entirely new industries or allow businesses to improve efficiency (increase profits and cut costs) and offer superior performance and customisation.

As we have already seen with Google's acquisition of Nest (cf. *infra sub* para. 2.2.) and Qualcomm's acquisition of CSR,[15] market players are already trying to realise the huge economic potential offered by the IoT, through big transactions.

---

[9] Smart meters identify, analyse and communicate electricity use from an individual residence to a utility company. They can reveal when a person is at home, cooking, showering, watching television or on vacation, and this information can be used to infer whether the resident is wealthy, clean, healthy or sleep-deprived. Cf. Balough (2011), 165; Stern (2011), 158; Murphy (2015), 191; Brown (2014), 172.

[10] For even more fascinating examples see Kominers (2012), 4; Barbry (2012), 84; Robinson (2015), 664; Kester (2016), 207.

[11] The phrase seems to have originated with Cisco's CEO John Chambers. See http://www.internetofeverything.cisco.com.

[12] Rose (2014), 11; Thierer (2015), 7.

[13] The IoT's impact on industry structure and the competitive transformation taking place are discussed in an enlightened and very informed manner by Porter / Heppelmann (2014).

[14] New data devices in the workplace capture and communicate employees' location, duration of breaks, productivity in completing their tasks and more. Cf. Cunningham (2014), 138.

[15] For further examples see Computer Technical Support in USA (2014), Top 10 Mergers and Acquisitions in The Internet of Things Space 2014, 3 September 2014, available at: https://computertechsupportinus.wordpress.com/2014/09/03/top-10-mergers-and-acquisitions-in-the-internet-of-things-space-2014-2/ and Yoshida (2014), Top 2014 Acquisitions that Advanced the Internet of Things, EE Times (12 November 2014), available at: http://www.eetimes.com/document.asp?doc_id=1324 935.

1.2 Industry Impact and Future Trends

This seamless web of connectivity and pervasive computing promises to usher in 'a third computing revolution'[16] or a 'fourth industrial revolution', or what has been called 'Industry 4.0',[17] and it will bring about profound changes that will rival the first wave of Internet innovation.[18]

While in 2015 the number of connected 'things' was a few billion, the most conservative predictions are that, by the end of 2020, over 20–25 billion devices will be connected as part of the IoT.[19] An economic impact of 3.9 trillion to 11.1 trillion dollars per year by 2025, which will represent up to 11% of the world's economy, has been estimated.[20]

2 The Role of Law in the IoT

Solutions developed by engineers, however, also need to be in compliance with existing regulations. Although legal interest is growing, most academic responses still come up from the technological, urban, environmental and sociological sectors rather than from the legal sector and have primarily laid emphasis on the benefits of IoT, rather than its challenges. This can primarily be explained by the fact that the intensity and magnitude of this technological revolution are mostly unknown to date.

---

[16] The first wave of IT, during the 1960s and 1970s, automated individual activities in the value chain. The second wave of IT-driven transformation, in the 1980s and 1990s, coincided with the advent of the Internet. This enabled coordination and integration across individual activities; with outside suppliers, channels and customers; and across geography. The first two waves, however, left products largely unaffected. Now, in the third wave, IT is becoming an integral part of the product itself. See Porter / Heppelmann (2014).

[17] The term originates from a project in the high-tech strategy of the German government and has been used by Chancellor Angela Merkel to identify 'the comprehensive transformation of the whole sphere of industrial production through the merging of digital technology and the Internet with conventional industry'. The term has been fully adopted by the EU Institutions. Cf. the EU Parliament's 2016 Study on Industry 4.0, prepared by Policy Department A and available at: http://www.europarl.europa.eu/RegData/etudes/STUD/2016/570007/IPOL_STU(2016)570007_EN.pdf.

[18] Lee (2014), Everything's Connected: How Tiny Computers Could Change the Way We Live, Vox (13 August 2014), available at: http://www.vox.com/2014/5/8/5590228/how-tiny-computers-could-change-the-way-we-live.

[19] Huawei Technologies Co., Ltd. (2015), Global Connectivity Index 2015, available at: http://www.huawei.com/minisite/gci/en/index.html.

[20] These trends are investigated in depth by the final report of the European Commission (2014b), 24-26, 61-62. Other estimations are reported by McKinsey Global Institute (2015), 2, 36. For a more comprehensive bibliography on the economic impact of the Internet of Things see Thierer (2015), 11.

As, in the past, the Internet has led us to adopt or rethink several bodies of law in order to address very different issues (from consumer protection in e-commerce sales, to ISP liabilities for tort of defamation or infringement of IP rights committed online), the IoT is going to be the next legal challenge. As it matures and becomes more complex day by day, the law may struggle to evolve quickly enough to address the challenges it poses.

2.1 Threat to Privacy: Passive Data Transmission

Many of the legal issues arising from smart devices relate to user privacy and device security.

In the coming years, we will handle apps able to obtain every kind of measurement on an ongoing basis. By now e-readers know what page you stopped reading on. Navigators display speed, direction and travel patterns of your car and will soon be able to drive it taking into consideration traffic jams, road-work, the best petrol prices or which service station has a tyre-replacement service or a McDonald's where you can have lunch.

The EU data protection law, also after the entry into force of the General Data Protection Regulation (GDPR), hinges on providing individuals with notice and obtaining their consent before collecting data. However, IoTs tend to collect data without users' awareness (of how much of their data is captured, who controls it and for what purpose).[21]

While technology rapidly advances and becomes ever more pervasive, the right to privacy is becoming ever more difficult to enforce. This has led some to argue that privacy will soon be a thing of the past, if we do nothing about it.[22]

The EU Commission addressed the issue with a 2009 Communication entitled *Internet of Things. An action plan for Europe*. Among the 14 lines of action laid down, it included the necessity for a 'continuous monitoring of the privacy and the protection of personal data questions'.[23] The Commission warned that failing to adopt a proactive 'privacy by design'[24] approach to IoT 'could place Europe in a

[21] Levin (2007), 229 and Willborn (2006), 976, 980, point out the difficulties of requiring employers to provide notice and obtain consent before monitoring their location, productivity and behaviour and highlight how that consent is often illusory: no consent, no job.

[22] Garfinkel (2000); Holtzman (2006); O'Hara / Shadbolt (2008); Whitaker (2000); Schermer (2007), 2010, more specifically argues that privacy will cease to exist in 20 years More optimistically, Froomkin (2000), 1543, concludes that all is not lost.

[23] European Commission (2009).

[24] It is the principle according to which privacy should be built into systems from the design stage, in such a way that privacy rules are automatically enforced as much as possible and that default settings should be adopted that restrict data collection, storage and sharing to the absolute minimum that is necessary for achieving the specified purposes of the system. This concept was developed by the Information and Privacy Commissioner of Ontario, Canada, Dr. Ann Cavoukian, who set forth the 7 Foundational Principles of Privacy by Design; see Cavoukian (2013), 175. Regulation

position where it is forced to adopt technologies that have not been designed with its core values in mind, such as the protection of privacy and personal data'.

As a follow-up, the EU Commission launched a 2012 consultation to solicit the views of stakeholders and the public at large on 'what framework is needed to unleash the potential economic and societal benefits of the IoT, whilst ensuring an adequate level of control of the devices gathering, processing and storing information'.[25] The results of the consultation were released as a Report in 2013.[26]

Based on the inputs provided by the European Commission, policymakers and commentators focused on how to adequately inform users on the processing of personal data and how to collect individuals' privacy consent.[27]

Given the difficulties in collecting traditional forms of consent, many commentators are moving away from notice and consent as a main mechanism for validating data collection. Users do not have the resources, opportunity, inclination or motivation to give meaningful consents in the current online environment. This seems to be true a fortiori within the IoT context.[28]

Other scholars argued that—instead of a broad privacy law that declares all personal data worthy of protection and that requires notice and consent before data collection—privacy law should narrowly target specific harms arising from specific privacy violations and regulate the use of sensitive data only in relation to these particular risks.[29]

(EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the movement of such data (General Data Protection Regulation) [2016] OJ L 119/1, embraces 'privacy by design' in Article 25. For an overview of the various challenges designers may need to engage with in the context of IoT see Urquhart / Rodden (2016), 5; Klitou (2014), 50.

[25] The public consultation was held between April and July 2012, see European Commission, Press Release (IP/12/360): Digital Agenda: Commission consults on rules for wirelessly connected devices – the 'Internet of Things', 12 April 2012. Also, the Italian Privacy Authority recently launched a consultation on the IoT, seeking inputs from the industry on how to regulate it: http://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3898743.

[26] The European Commission published the public consultation's results at: https://ec.europa.eu/digital-single-market/en/news/conclusions-internet-things-public-consultation.

[27] This issue seems to be much debated where data is collected in public, as in the context of the 'smart cities'. In this case, difficulties arise from the traditional standpoint that privacy law applies to private zones, focused on the body, the home and private communications. A growing body of literature deals with the potential threat the IoT poses to privacy in the smart-city context. See Koops (2014), para. 3, redefining the 'boundaries of private spaces', arguing that 'place is no longer a useful proxy to delineate the boundaries of the private sphere'; Weber / Weber (2010), 39.

[28] See McDonald / Cranor (2008), 540; Arnold / Hillebrand / Waldburger (2015), 64, considers that reading a privacy policy might take longer than the actual length of interaction with the IoT device, reducing further the incentive to read.

[29] This 'regulatory approach' to the field of risk management has been proposed by Spina (2014), 248 and Cunningham (2014), 144, according to whom 'Privacy laws that turn on personal information and that require notice and consent before data collection poorly reflect the technological landscape and remain impractical at best. Privacy laws should focus on data use, not collection'.

The U.S. Federal Trade Commission (FTC), on the other hand, has come up with a range of possible approaches to getting consent[30] by ways and methods more tailored to the new digital environment: for instance, (1) directing customers to privacy settings pages or 'management portals'; (2) putting quick response (QR) codes[31] on IoT devices; (3) providing different icons to convey privacy-related information.[32]

The general feeling is that the industry sector needs more certainty on applicable obligations. An investigation run by the Global Privacy Enforcement Network, the international network established to strengthen cooperation among 26 privacy authorities, reached the conclusion that over 60% of the reviewed IoT technologies are not fully privacy compliant with data protection laws.[33]

The Italian data protection authority commented on the results that the lack of compliance is expected to impact consumers' trust.[34] The same uncertainty, however, might potentially impact on the supply side and delay the development of IoT technologies due to the potential legal risks or the excessive burden imposed by current privacy regulations.[35]

A first step in this direction has been the adoption in September 2014 of the Article 29 Working Party Opinion on the Internet of Things, which proposes a set of recommendations for stakeholders to comply with the current EU data protection legal framework.[36] The Opinion identifies various stakeholders potentially involved in processing data from IoT devices: device manufacturers; device lenders or renters; application developers; social media platforms; and data brokers. Each of these stakeholders may be qualified as a data controller for the purposes of the application of the EU data protection rules.[37] In this Opinion, the Working

[30] See FTC (2015), 48, which also makes recommendations on data minimisation in terms of the amount of consumer data collected, as well as the length of retention. The report also recommends that companies notify consumers and give them choices about how their information will be used, particularly when the data collection is beyond consumers' reasonable expectations.

[31] A QR code is a two-dimensional matrix that can be converted to information via smartphones with built-in cameras, thanks to over 1,500 smartphone applications to give them easy access to privacy policies.

[32] Such as that the IoT device is connected to the Internet or different levels of risk and/or different types of data collection. See Edwards / Abel (2014), who raise issues of recognisability, confusion, global standardisation and interoperability.

[33] This action is part of the 'Privacy Sweep 2016'. Out of 300 reviewed devices, 59% do not provide adequate information on how personal data is collected, used and communicated to third parties; 68% do not provide appropriate information on the modalities of storage of data; 72% do not explain to users how their data can be deleted from the device; and 38% do not guarantee easy-to-use modalities of contact for clients that are willing to obtain clarifications on privacy compliance.

[34] See http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5443681.

[35] For a more comprehensive overview on the privacy problems of these new technologies see Thierer (2015); Peppet (2014); Edwards (2016); Maras (2015); Weber (2015). For a comparison between the U.S. FTC and the Article 29 Working Party approach see Leta Jones (2015), 648.

[36] Article 29 Working Party (2014).

[37] More precisely, the implementing provisions of one or more Member States apply whenever personal data is processed 'in the context of the activities of an establishment' of the data controller

Party recalls the obligations to inform users of the characteristics and purposes of the data processing before commencing it, not only the device user but all those who are in the 'geographical or digital' vicinity when data relating to a certain device is collected. The Opinion has been criticised for presuming that individuals are in control of their personal data, even if such control may not always be feasible.[38]

Attention to the privacy's concerns around Iot technologies has been paid also by the Working Party 29 Guidelines on the requirement of a Data Protection Impact Assessment (DPIA), which expressely mention "certain IoT applications" as an example of "innovative technological or organisational solution" which could have a significant impact on individual's daily lives and privacy and therefore trigger the need to carry out a DPIA.

2.2 Property Interest in 'Big Data' and Market Power Based on Data Ownership: The Intersection of Big Data and Antitrust Law

Another interesting legal issue is connected to the ownership of data that flow through the IoT.[39]

As mentioned, connected products are collectors of information. Control over them is now increasingly possible thanks to the development known as 'big data', which refers to gigantic digital datasets extensively analysed using computer algorithms.[40]

When they are able to exploit the information collected from users, IoT companies can create economic value and generate new business opportunities by optimising their products, individualising marketing and pricing and best meeting customers' demands.[41] Many of the world's most valuable companies owe much of their success to the amount and quality of personal data under their control and the innovative ways in which they can use them. Not surprisingly, personal information

in the territory of that State, or in all cases where the data controller is established outside the EU, but makes use of 'equipment' situated in that territory. This amounts to saying that their application is provided in very broad situations.

[38] Eskens (2016), 3; Manning (2016), 3, warning that, despite the confidence of the Working Party, big data poses challenges that may prove insurmountable for the existing legal framework.

[39] See Ciani (2017) and (2018).

[40] See Article 29 Working Party (2013), 35. The European Commission (2014a), 4, defines the term 'big data' as 'a large amount of different types of data produced with high velocity from a high number of various types of sources'. According to McKinsey Global Institute (2011), 1, big data means 'datasets whose size is beyond the ability of typical database software tools to capture, store, manage, and analyse'.

[41] This has largely proved to be true for online service providers, such as search engines, given their ability to use personal data they may have acquired, in terms of more relevant search results and more targeted advertising. On the critical importance of the acquisition of personal data for most key Internet players see Geradin / Kuschewsky (2013), 2.

has been compared to currency[42] and dubbed the 'new oil' of the information economy; there is broad consensus recognising in them a clear economic value.

This data can have an enormous impact on market power and even lead to anti-competitive concerns by creating or strengthening a dominant market position.[43]

How to measure the control of personal information for this purpose promises to be a challenging issue. Normally the Commission evaluates market power through an assessment of market share, depending on company turnover. By reference to data on traditional sales or volume, however, a relevant market share held by a provider of a free online service cannot easily be calculated.

Such a 'purely economic approach'[44] was applied to the *Google-DoubleClick* merger.[45] DoubleClick was an online advertising company specialising in the serving and tracking of online ads by using cookies. The Commission concluded that the combination of the two undertakings' databases on customer search and web-browsing behaviour would not create 'a competitive advantage in the advertisement business that could not be replicated by other players that have access to similar web-usage data'.[46]

This decision had the full merit of drawing attention to the relationship between competition and privacy. Many thereupon expressed the concern that the Commission failed to properly consider how the merger could give the combined entity greater potential to track online consumer behaviour and use information for targeting purposes by merging the two companies' datasets.[47]

---

[42] See recital 13 of the Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, COM(2015) 6434 final, which states: 'In the digital economy, information about individuals is often and increasingly seen by market participants as having a value comparable to money. Digital content is often supplied not in exchange for a price but against counter-performance other than money i.e. by giving access to personal data or other data'. For a survey of methodologies for measuring the value of personal data from a purely monetary perspective (i.e. without taking into account the indirect impacts of the use of personal data on the economy or society), see OECD (2013), 18. *Contra* Lambrecht / Tucker (2015), 158, who suggest that big data is unlikely to be valuable if it is not inimitable or rare and substitutes exist.

[43] One of the first attempts to address the limits placed by EU competition law on the acquisition and processing of personal data may be attributed to Geradin / Kuschewsky (2013).

[44] The European Data Protection Supervisor (2014) critics this approach for failing to consider whether the combined entity should process search and browsing data for purposes incompatible with data protection law.

[45] European Commission, Case No. COMP/M.4731, *Google/DoubleClick*, 11 March 2008.

[46] Also, the FTC on 20 December 2007 voted to approve the merger, finding no concerns with regard to competition (cf. https://www.ftc.gov/enforcement/cases-proceedings/071-0170/proposed-acquisition-hellman-friedman-capital-partners-v-lp). See also Edwards (2008), 31 pointing at the need for inclusion of issues of data privacy/protection as a part of future merger reviews.

[47] This was the point of Commissioner Pamela Jones Harbour, in her Dissenting Statement in the matter. See also Hahn / Singer (2008), 3: 'The first concern is that Google may accumulate so much consumer data—which can be used to more effectively target advertising—that it may reach a tipping point that limits new entrants into the online advertising market. This concern suggests that new entrants would not have comparable consumer information, and thus would begin at a significant competitive disadvantage to Google'; Nathan (2014) 854, details how understanding

On the other side of the Atlantic, the issue of data monopolies was discussed in relation to Google's acquisition of Nest Lab, a smart device mostly known for its learning thermostats. While the FTC cleared the merger with an early termination notice, some observers outlined the risk that Google would strengthen its dominant position in the search advertising market by accessing the data gathered.[48]

Commentators generally split into two camps: one in favour of more proactive antitrust enforcement in the big data realm, and one opposing such intervention, considering antitrust inappropriate for the regulation of big data.[49]

The opinion that closer dialogue between regulators will lead to more effective regulation is shared by the European Data Protection Supervisor (EDPS) in its preliminary opinion of March 2014 on privacy and competitiveness in the age of big data.[50]

The EDPS warned that if regulators fail to acknowledge the increasing importance of personal information as an intangible asset, more and more services reliant on big data could in effect be left uncovered by competition rules. As a result, the Opinion lays the ground for allowing data protection and competition law to be merged so far that privacy policies could become a parameter of competition.

In this direction, the German Bundeskartellamt and the French Autorité de la concurrence[51] on 10 May 2016 published a joint Report on Competition Law and Data[52] that calls for a case-by-case assessment of competition law risks resulting from companies with a significant 'data advantage'. In particular, the Report identifies as relevant when assessing the data's contribution to market power: (1) whether the data under consideration can easily be obtained by rivals and (2) whether the scale and scope of data matter.

The first case for applying this approach arose from the Bundeskartellamt itself. On 2 March 2016, it started an investigation against Facebook, alleging the company to have abused its dominant position by imposing unfair trading terms on consumers as to the amount of data it captures about them by using third-party

---

the dynamics of data mining and behavioural targeting reveal the clear harm to consumers from Google's monopoly of the online search advertising market. Abramson (2008) 655, examines whether there is a distinct 'Internet market' and how an antitrust analysis of such a market should differ from parallel analyses applied to more conventional markets.

[48] See https://www.ftc.gov/enforcement/premerger-notification-program/early-termination-notices/20140457.

[49] For a review of scholarly works on the implications of Big Data on competition see Sokol / Comerford (2016), 271, who critique the suggested potential harms to competition from Big Data and suggest that antitrust law is ill-suited to police Big Data and its use by online firms. The same opinion is shared by Lerner (2014), 46, suggesting that real-world evidence indicates that such concerns are unwarranted for many online businesses. See also articles posted on https://www.competitionpolicyinternational.com/may-152/.

[50] European Data Protection Supervisor (2014), 33, 37.

[51] One month before the publication of the results of the joint study, the President of the French Competition Authority announced that a sector inquiry would be started soon regarding the overlap between big data and competition law, which may potentially result in the opening of proceedings against actors in the data sector.

[52] Autorité de la concurrence and Bundeskartellamt (2016).

websites, including services owned by Facebook itself as WhatsApp or Instagram.[53] On December 2017, a preliminary assessment has been issued, assuming that Facebook is dominant on the German market for social networks. The move of the German Authority against Facebook is the first attempt to apply a 'data-based approach' (i.e. the amount of user data collected or the number of users) in order to assess the market power of data-driven business.[54] The German legislator has acknowledged this approach and in § 18(3a) of the German Competition Act made access to personal data a criterion for assessing market power.

Building upon its 2014 Opinion the EDPS published on 23 September 2016 a second opinion on the coherent enforcement of fundamental rights in the age of big data.[55] In order to support the current trend for synergies between fields of law, it suggested the creation of a digital clearing house: a voluntary network of regulatory authorities at national and EU level aimed at mutually enhancing their respective enforcement activities. The clearing house would be responsible for issuing advice on the most appropriate regulatory solution, which could be adopted for each case submitted to its scrutiny.

At last, during the Brussels EDPS–BEUC Conference on Big Data, on 29 September 2016, Commisioner Vestager echoed some of the points raised by the EDPS. She confirmed that the Commission 'is exploring whether we need to start looking at mergers with valuable data involved, even though the company that owns it doesn't have a large turnover'.

She also noted that 'the competition rules weren't written with big data in mind' and hinted that a proposal for a new Directive might be on the table of the EU institutions next year.[56]

3 Protecting and Enforcing IoT Technologies Through Intellectual Property Rights

The IoT's great potential to improve efficiencies and allow businesses to both increase profits and cut costs brings as a logical consequence the desire of manufacturers to protect smart object from misappropriation by competitors. Intellectual property rights can, of course, serve this purpose. Smart objects can be protected through patents, copyright or trade secrets. Furthermore, copyright and database protection can be used to control the use in an IoT application of data or data structures.[57]

---

[53] Bundeskartellamt, Press release: Bundeskartellamt initiates proceeding against Facebook on suspicion of having abused its market power by infringing data protection rules, 2 March 2016.

[54] Further information on the Facebook proceeding are available at this link https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Diskussions_Hintergrundpapiere/2017/Hintergrundpapier_Facebook.html;jsessionid=B070B6AEBD14686C7183C5A2C15F7570.1_nn=3600108.

[55] European Data Protection Supervisor (2016).

[56] https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/big-data-and-competition_en.

[57] See Ciani (2017).

3.1 Patents

A significant amount of patenting activity concerns the core technologies of IoT. Categories of potential inventions includes smart objects, communication protocols between smart objects[58] and software that will process data collected by them and translate it into useful and actionable intelligence.

Samsung has filed a patent for a wearable device controlled by wrist gestures.[59] Google has received a patent on making 'heart gestures' in conjunction with a head-mounted display that can recognise this gesture and post its content to social media along with 'an indication that the image is liked'.[60]

Google has also filed a patent for technology that would allow drivers to control many functions of a vehicle with hand gestures. The system utilises a depth camera mounted on the roof of the vehicle and a laser scanner. If a driver wanted to roll down the window, adjust volume of the radio or change stations, he or she would make respectively a swiping or a turning motion near the window or the radio.[61]

Computer programs are on the list of subject matters that are explicitly excluded from patent protection (Art. 52(1) of the European Patent Convention), but this exclusion applies only if the protection is demanded for software 'as such', with no technical teaching. On the contrary, a patent can be granted if the software constitutes an invention that is susceptible of industrial application.[62]

The first studies on the patent landscape of the IoT showed that up to the year 2009 the number of patent filings in this domain saw a slow but constant rise (with 427 patents being filed by 228 patent filers in 2009). A steep rise occurred from the year 2010, when the number of patents filed rose to 1036.

---

[58] For example, 6LoWPAN is an Internet protocol that optimises the Internet for low power, low bandwidth devices. Another protocol, known as Bluetooth Low Energy (BLE), is designed to allow devices to consume small amounts of energy and save the battery life of mobile devices.

[59] See http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%2220140143785%22.PGNR.&OS=DN/20140143785&RS=DN/20140143785.

[60] See Mead (2013), Google Patented the 'Heart' Gesture and other Fun Hand Moves, Motherboard (16 October 2013), available at: http://motherboard.vice.com/blog/google-patented-the-heart-gesture-and-other-fun-hand-moves.

[61] See Strong (2013), Google wants you to gesture when you drive (but not THAT gesture), NBC News (9 October 2013), available at: http://www.nbcnews.com/tech/innovation/google-wants-you-gesture-when-you-drive-not-gesture-f8C11363368.

[62] See EPO Board of Appeal, T 258/03, Auction Method/Hitachi, ECLI:EP:BA:2004:T025803.20040421 and Guidelines for Examination in the European Patent Office, Part G, Chapter II-3, section 3.6 'Programs for computers', 20 June 2012. In the U.S., courts have been very wary to say that software is patent-eligible. For example, the Supreme Court has held that a process claim embodying an algorithm for converting binary-coded decimal numbers into pure binary numbers was patent-ineligible [Gottschalk v. Benson, 409 U.S. 63, 71-72 (1972)]. The test applied by the Supreme Court was established in *Alice Corp. Pty. v. CLS Bank Int'l*, 134 S. Ct. 2347, 2355 (2014). In this case, the Supreme Court denied patent protection to a process claim directed to the concept of intermediated settlement, specifying that simply requiring generic computer implementation of that abstract idea did not make the idea patent-eligible.

The geographical distribution of the patent set in the field of IoT allows the observation that most patents are filed in the United States, but countries like China, South Korea, Canada, Taiwan and Japan also show extensive patent filing. LG, with 482 patent filings, is the top filer, with Ericsson taking the second spot with 404 patent filings.

The distribution of patents is very fragmented, with the top filer having around 5% of the total filings. Amongst big players, some non-practicing entities (NPEs)[63] like Interdigital and ETRI also have high patent filings in IoT.[64]

This is clear evidence of high chances of patent litigation in this domain in the near future.[65] Indeed, the recent spate of litigation that has occurred in the smartphone industry was caused by Microsoft, Apple and Google mainly because of the fact that many of the owners of 3G and LTE patents are not manufacturers but rather the so-called trolls.[66]

3.2 Software

A second type of protection for software applications is offered by copyright law.

Scholars have debated for decades how much legal protection software developers should get from copyright law to induce optimal levels of investment in the development of computer programs and, at the same time, not impede beneficial standardisation.[67] This delicate balance continues to be hard to find.

---

[63] NPEs are firms that do not produce goods, but rather acquire patents in order to license them to others.

[64] Lexinnova (2014).

[65] Actually a round of patent lawsuits seeking to assert intellectual property rights has already started in the U.S., between Jawbone and Fitbit, the leading players in the growing market for fitness trackers. Before the Delaware District Court, Case No. 1:15-CV-00990, Fitbit alleged infringement of three of its patents, U.S. Patents No. 8,920,332 (titled *Wearable Heart Rate Monitor*); No. 8,868,377 (titled *Portable Monitoring Devices and Methods of Operating Same*); and No. 9,089,760 (titled *System and Method for Activating a Device Based on a Record of Physical Activity*). According to the complaint, Jawbone's products associated with components of its UP series of trackers indirectly infringe the patents at issue. Two earlier patent infringement complaints were filed in the Delaware District Court and in the District Court for the Northern District of California in September 2015. Jawbone earlier filed three lawsuits in an attempt to prevent Fitbit from importing or selling its fitness trackers. The whole saga is described by Spence (2016).

[66] A patent troll, instead of creating new products or coming up with new ideas, buys up patents cheaply from companies down on their luck, and then uses them as legal weapons, starting litigation or even just threatening to, with the aim to monetise. For an explanation of why FRAND disputes are particularly consistent in the smartphone realm see Lim (2014), 14.

[67] Extensive literature has been produced about copyright protection for computer programs. See, e.g., Nimmer / Bernacchi / Frischling (1988), 625; Ginsburg (1994), 2559; Menell (1989), 1045; Miller (1993), 977; Reichman (1989), 639; Samuelson / Davis / Kapor / Reichman (1994), 2308.

According to Directive 2009/24/CE of 23 April 2009 (Software Directive), computer programs can be protected in any form of expression as literary works, subject to the requirement of originality. The originality threshold is hard to satisfy where functional constraints and industry standardisation limit the possible author's imprint. Both the *SAS Institute, Inc. v. World Programming Ltd* decision[68] and the prior ruling in *Softwarová*[69] seem to confirm this view, rejecting the idea that programming language, data formats and graphic user interfaces could be protected under the Software Directive,[70] as they do not constitute a form of expression of the program.[71]

For more than 20 years, U.S. case law has shown a strong consensus that program interfaces necessary for interoperability are unprotectable by copyright law.[72] This finding, however, was recently called into question by the Court of Appeals for the Federal Circuit (CAFC) in *Oracle Am., Inc. v. Google Inc.*[73]

[68] ECJ, SAS Institute, C-406/10, ECLI:EU:C:2012:259. For comments see Nickless (2012); Onslow / Jamal (2013); Barker / Harding (2012); Marly (2012).

[69] ECJ, Bezpečnostní softwarová asociace, C-393/09, ECLI:EU:C:2010:816. For comments see Lindhorst (2011); Marly (2011); Smith, L. J. (2011).

[70] On this outcome See Samuelson / Vinje / Cornish (2012), 166 explaining why the text and legislative history of the EU Software Directive, in line with international treaty provisions, should be understood as providing protection only for the literary aspects of programs, but not to their functional behaviour, programming languages and data formats and interfaces, which are essential for achieving interoperability.

[71] Nonetheless, the Court did not exclude the applicability of traditional copyright protection to these programmers' choices. According to Zingales (2015), 11 'while data and user interfaces are substantially different from APIs, these cases would appear to offer ground for reaching the conclusion that choices for interfaces concerning the implementation of abstract ideas contained in the source code can be sufficiently original, as were deemed to be those concerning languages or formats'.

[72] In *Computer Associates Int'l, Inc. v. Altai, Inc.*, 982 F.2d 693 (2d Cir. 1992), the Second Circuit Court of Appeals invited courts to 'filter' out unprotectable elements of programs, such as those necessary for achieving interoperability with other programs, before assessing infringement claims (so-called abstraction-filtration-comparison, or AFC test). The Altai approach has been endorsed in numerous other circuit court decisions. For more references, see Lemley (1995), 12 treating *Altai* as the leading case on copyright protection for computer programs. Other landmark decisions were *Lotus Dev. Corp. v. Borland Int'l, Inc.*, 49 F.3d 807, 814-15 (1st Cir. 1995), ruling that the command hierarchy of a spreadsheet program was an integral part of a method of operation, expressly excluded by law from the scope of copyright protection in programs and *Lexmark Int'l, Inc. v. Static Control Components*, 387 F.3d at 541-42, in which the Sixth Circuit established that a computer program embedded in Lexmark's printer cartridges that competitors had to install in order to make their cartridges interoperable with Lexmark printers was uncopyrightable.

[73] *Oracle America, Inc. v. Google Inc.,* 872 F.Supp.2d 974 (N.D. Cal. 2012), rev'd, 750 F.3d 1339 (Fed. Cir. 2014), cert. denied, S.Ct. (2015). For a summary of the *Oracle v. Google* saga and its legislative and jurisprudential background and for critiques of the Federal Circuit's decision see Menell (2017), 31, 42 and Samuelson (2015), 702.

At issue was whether Google infringed Oracle's copyright when replicating the Java APIs[74] in the implementation of the Android OS. Interests at stake were significant.

A final determination that Oracle could claim a copyright on Java APIs could have had an adverse impact on the development of interoperable systems. Indeed, this would have allowed copyright holders to control companies' ability to develop their own programs to be compatible with other platforms.

The CAFC reversed the ruling by Judge William Alsup of the Northern District of California[75] that APIs are not subject to copyright. The CAFC treated patents and copyrights as providing overlapping protection for computer program innovations. The U.S. Supreme Court decision not to review the CAFC ruling[76] left this finding intact.

However, the case returned to Judge Alsup's district court for a jury trial focused on Google's fair-use defence. In May 2016, the jury unanimously agreed that Google's use of the Java APIs 'constitutes a fair use under the Copyright Act'.[77] Oracle appealed the retrial.

On March 27, 2018, the U.S. Court of Appeals for the Federal Circuit[78] reversed the retrial's decision, concluding that Google's use of the Java API packages was not fair and violated Oracle's copyrights. Google's commercial use of the API packages weighed against a finding of fair use. Google merely copied the material and moved it from one platform to another without alteration, not a transformative use. The court remanded for a trial on damages, but Google may still appeal to the Supreme Court.

3.3 Trade Secrets

Subject to the fulfilment of the criteria of confidentiality, commercial value and reasonable efforts of confidentiality's maintenance, IoTs can be subject to trade secrets protection, provided by the European Union's new Directive approved by the European Council on 27 May 2016[79] (Trade Secrets Directive).

---

[74] To understand Java's development and success see Menell (2017), 16.

[75] *Oracle America, Inc. v. Google Inc.,* 810 F.Supp.2d 1002 (N.D. Cal. 2011). While acknowledging that the overall structure of the Java API packages is creative and original, Judge Alsup nonetheless concluded that it functions as 'a command structure, a system or method of operation–a long hierarchy of over six thousand commands to carry out pre-assigned functions'.

[76] *Google, Inc. v. Oracle America, Inc.*, 135 S.Ct. 2887 (2015).

[77] *See* Special Verdict Form (Document 1928-1, *Oracle America, Inc. v. Google Inc*. 3:10-cv-03561-WHA).

[78] See Oracle America, Inc. v. Google, Inc., no. 17-1118 (Fed. Cir. 2018).

[79] It remedied the lack of specific EU-level regulation on the protection of trade secrets. Before, common standards were imposed only at the international level for all WTO Members by Article 39(2) of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs). The Directive brought the adoption of a shared definition of trade secrets across the EU. It is based on the common constitutive elements of protection across various member States, specifically: (i) the information must be confidential; (ii) it should have commercial value because of its confidentiality; and (iii) the trade secret holder should have made reasonable efforts to keep it confidential.

Due to the difficulty of qualifying for patent protection and the thin scope covered by copyright protection, trade secrets represent a valuable and concrete opportunity for software developers.

3.4 Database Protection

Sets of data collected by IoT devices could be protected as a database[80] according to Directive 96/9/EC (Database Directive).

Such rights are of two types: Article 4(1) of the Directive grants copyright protection to those databases which, by reason of the selection or arrangement of their contents, meet the low threshold of originality set by the European Court of Justice.[81]

A second kind of protection (called sui generis) grants the database makers the right to prevent extraction and/or re-utilisation[82] of the whole or of a substantial[83] part of its contents, upon showing the existence of a substantial investment in their obtainment, verification or presentation (Article 7 of the Directive).[84]

3.5 Technical Protection Measures

Due to the easy duplicability of information transmitted in digital form, copyright owners regularly resort to technical protection measures (TPMs), such as encryption, to prevent acts which are not authorised by the right holder of copyright or other related rights.[85]

---

[80] Article 1.2 of the Database Directive defines 'database' as: 'a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means'. Recital 17 of the Database Directive further states that 'the term "database" should be understood to include literary, artistic, musical or other collections of works or collections of other material such as texts, sound, images, numbers, facts, and data'.

[81] ECJ, Infopaq International, C-5/08, ECLI:EU:C:2009:465. For more comments see Derclaye (2010).

[82] 'Extraction' is defined by Article 7(2)(a) of the Database Directive as 'the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form'; in turn, 're-utilisation' refers to any 'form of making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, by on-line or other forms of transmission'.

[83] Article 7(5) extends protection against extraction and re-utilisation beyond the substantiality threshold, reaching the 'repeated and systematic extraction and/or re-utilization of insubstantial parts of the contents of the database implying acts which conflict with a normal exploitation of that database or which unreasonably prejudice the legitimate interests of the maker of the database'.

[84] In this regard, the ECJ has clarified that, when determining if there is a 'significant investment' in a database, any investment in the creation of the material making up the content of the database must be disregarded. See ECJ, British Horseracing Board Ltd., C-203/02, ECLI:EU:C:2004:695. For interesting remarks on this decision see Aplin (2005); Masson (2006).

[85] The definition of TPM is established in Article 6(3) Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society (InfoSoc Directive),

The legal system reinforces this type of protection by outlawing not only any acts of circumvention of TPMs,[86] but also the manufacturing and sale of devices whose primary purpose or effect is to enable such circumvention.[87]

Consoles and video games are a classic example of complementary goods generating lock-out strategies: by embedding copyrighted software into its consoles, the producer ensures that only original cartridges (containing the code for that particular console) can be played.[88] This strategy has led to widespread deployment of electronic devices ('modchips') that disable the encryption mechanisms embedded in the console, thereby enabling the interoperability of video games made or distributed by unauthorised developers.[89] The European Court of Justice addressed the issue of whether modchips should be considered circumvention devices forbidden by Article 6(2) of the Copyright Directive in *Nintendo and Others v. PC Box*.[90] The decision established that the legal protection offered by Member States must comply with the principle of proportionality, not prohibiting devices or activities which have a commercially significant purpose or use other than circumventing a TPM for unlawful purposes. This test allows defendants to show that a particular TPM is misused, as long as its goal is primarily to prevent third-party applications from gaining access to the platform, rather than merely preventing the use of 'pirated' copies of video games and provided that less intrusive alternatives are available for a comparatively effective copyright protection.

---

referring to 'any technology, device or component that, in the normal course of its operation, is designed to prevent or restricts acts … which are not authorised by the right holder of any copyright or any right related to copyright'.

[86] Article 6(1) of the InfoSoc Directive states that '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."

[87] Article 6(2) of the InfoSoc Directive states that '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'. Furthermore, Article 7.1(c) of the Software Directive states 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 unauthorised removal or circumvention of any technical device which may have been applied to protect a computer program'.

[88] Zingales (2015), exploring in depth the adoption of lock-in strategies in the video-games sector.

[89] Several jurisdictions recognise possession and sale of modchips as a crime. See for instance Article 171 ter, para. 1, lit. F bis Italian Copyright Law (Law of 22 April 1941 n. 633).

[90] ECJ, Nintendo and others, C-355/12, ECLI:EU:C:2014:25. For further remarks see Newton / Moir / Montagnon (2014), 456. In Italy, the same principle was established by a decision of the Court of Rome, 10 October 2010, Nintendo CO. Ltd., Nintendo of America Inc., Nintendo of Europe GmbH v. Inter Media Trade Srl.

4 The Value of and the Obstacles to Interoperability

As in other areas of law, tools devised for protecting intellectual property rights may be abused, in particular by extending protection beyond its intended scope.[91] This concern may also affect the IoT context.

If an IoT object achieves interconnection with another through the use of a computer program that is protected by copyright or patent, the manufacturer of that object needs to rely on this program to render its object able to communicate with other technologies so that each can understand the other's data (so-called interoperability).[92]

As a result, in order to produce an object that is interoperable with technologies already on the market, a competitor is required to either obtain a licence for the protected content he intends to reproduce, or else meet the conditions for the application of one of the exceptions to the exclusive right. Otherwise he may be found liable of their infringement.

However, a company producing multiple IoT devices may have a strong interest in preventing third parties from relying on its exclusive rights in order to impede potential manufacturers of competing products from entering the market.

This could take place by the licensor refusing to grant a licence or by requiring unreasonable terms for licensing.[93]

By limiting the interoperability of their own technologies with devices manufactured by competitors, a company may succeed in building its own proprietary network and locking users into a closed branded 'ecosystem'.[94] Lock-out strategies

[91] The evolution of this transversal overprotectionist trend in IP law, to the point of reaching a 'misappropriation explosion' [Gordon (1992), cited], has been comprehensively described by Ghidini (1995), (2010), 19, and (2015), 32, who shows how the reaction has been mainly entrusted to the link between intellectual property and competition. See also Reichman (1993), 119, who warns that the intellectual property system '*risks collapsing of its own overprotection weight*'.

[92] The Software Copyright Directive, at Recital 10, defines interoperability as '*the ability to exchange information and mutually to use the information which has been exchanged*'. Zingales (2015) 6, distinguishes two levels of interoperability. While infrastructural interoperability enables IoT devices to exchange data under common network protocols, data interoperability concerns more directly users and developers of IoT applications, allowing them to meaningfully connect the interfaces of those applications. At the infrastructure layer, interoperability is achieved through the use of common protocols for the conversion, identification and logical addressing of data to be transmitted over a network. The most common standards in this layer are Ethernet and TCP/IP. At the application (upper) layer, interoperability is attained by reading and reproducing specific parts of computer programs, called Application Programming Interfaces (API), which contain the information necessary for third-party applications to run programs in a compatible format and without a loss of functionality. Differently from APIs, where specific interoperability information is required for the connection and execution of interoperable programs, data interoperability may also be obtained *ex post*, by exporting the output of the program and converting it into a readable format.

[93] The ability of a holder of an SEP to demand more than the value of its patented technology and to attempt to capture the value of the standard itself is referred to as patent 'hold-up'.

[94] Customers are said to be locked into a firm's product or service when the costs or disadvantages of switching a product or service are high, thereby discouraging customers to change.

may also serve as a mechanism of quality control of the products in the secondary market. Otherwise, the low value of substitutable products sold by third parties would risk disrupting the 'virtuous circle' of indirect network effects[95] and drive customers away from the base product.

However, since the nature of IoT technology is interactive, collaborative and entirely based on communication between two or more smart objects, lock-in strategies generate consumer dissatisfaction with those products that cannot be used to communicate with other brands' connected devices.[96] Meanwhile, incentives for potential competitors to enter the market are diminished because they are unable to attract a critical mass of users in order to compete.[97] On this basis, there is broad consensus on the fundamental value of connectivity and interoperability for inclusion in economic progress in this evolving technological environment.[98]

4.1 Legal Tools to Safeguard Interoperability

As mentioned above, legal provisions can be used to prevent technical interoperability by securing legal protection against acts of misappropriation. This range of tools to prevent interoperability should be balanced with 'pro-competitive antibodies'[99] that reduce the negative impact of exclusive rights and promote consumer welfare and innovation effects of interoperability. Without them, two things would happen: market players would implement strategies aimed at foreclosing interoperability with competitors' technologies (horizontal interoperability) and preventing third parties from building on their technology (vertical interoperability), and the legal system would only encourage situations of monopoly and underinvestment in the affected market.

On these grounds, IP law creates a specific framework under which the welfare elements of interoperability may be considered.

---

[95] Direct network effects arise if each user's payoff from the adoption of a good, and his incentive to adopt it, increase as more other users adopt it. For example, telecommunications users gain directly from more widespread adoption, and telecommunications networks with more users are also more attractive to non-users contemplating adoption. Indirect network effects arise if adoption is complementary because of its effect on a related market. For example, users of hardware may gain when other users join them, not because of any direct benefit, but because it encourages the provision of more and better software.

[96] Menell (2017), 4, points out that 'Building on and interoperating with widely adopted software platforms is the lifeblood of Internet age computing and commerce'.

[97] Gasser / Palfrey (2007), 12, conclude that interoperability generally supports innovation in the ICT context, but that the relationship between the two is highly complex and fact-specific.

[98] This perception of economic, socio-political and technical benefits flowing from open standards has garnered support within industry, academic and policymaker circles. See, for instance, Berkman Center for Internet & Society (2005).

[99] This expression has been very effectively used by Ghidini (2006), 7.

4.1.1 Software

The EU Software Directive contains a specific limitation to the ability to rely on software protection in order to prevent interoperability with other computer programs. Article 6(1) establishes the so-called decompilation exception for those acts of reproduction of the code and translation of its form that are

> indispensable to obtain the information necessary to achieve the interoperability of an independently created computer program with other programs, provided that the following conditions are met: (a) those acts are performed by the licensee or by another person having a right to use a copy of a program, or on their behalf by a person authorised to do so; (b) the information necessary to achieve interoperability has not previously been readily available to the persons referred to in point (a); and (c) those acts are confined to the parts of the original program which are necessary in order to achieve interoperability.

Furthermore, Article 5(3) of the EU Software Directive entitles the rightful owner of a copy of a computer program to observe, study or test the functioning of the program in order to determine the ideas and principles which underlie any element of the program ('black box testing'), provided he does so while performing any of the acts of loading, displaying, running, transmitting or storing the program which he is entitled to do.

4.1.2 Patents

It is possible that interoperability information resulting from reverse engineering or decompilation turn out to be protected by patents. In such a case, patent owners could still prevent the use of their patents for impeding interoperability.

For this reason, it has been proposed to introduce an interoperability exception for patents, mirroring that already existing in the Software Copyright Directive.[100]

The Agreement on a Unified Patent Court already provides for such an exception under Article 27(k), according to which the rights conferred by European patents with unitary effect under Regulation (EU) No 1257/2012 (Unitary Patent Regulation) do not extend to 'the acts and the use of the obtained information as allowed under Articles 5 and 6 of Directive 2009/24/EC, in particular, by its provisions on decompilation and interoperability'.

The Unitary Patent has shed new light on the interoperability issue. Article 8 of the Regulation further establishes that a 'proprietor of a European patent with unitary effect may file a statement with the EPO to the effect that the proprietor is prepared to allow any person to use the invention as a licensee in return for appropriate consideration'.

The filing of this statement is encouraged by Article 11.3 of the same Regulation, which provides for a reduction of the renewal fees, subject to the receipt of the statement.

[100] European Commission (2013).

4.1.3 Trade Secrets

Similar to the EU Software Directive, specific carve-outs are provided for 'reverse engineering' pursuant to Article 8 of the Trade Secrets Directive. This provision states that in no case can national legislation consider as unlawful the acquisition of information through (a) independent discovery or creation; (b) observation, study, disassembly or test of a product or object that has been made available to the public or that is lawfully in the possession of the acquirer of the information; (c) exercise of the right of workers' representatives to information and consultation in accordance with Union and national law and/or practices; and (d) any other practice which, under the circumstances, is in conformity with honest commercial practices.

Recital 39 clarifies that this provision does not affect the application of Article 6 of the Software Directive. This means that reverse engineering of a software protected under copyright law is allowed only for the limited purposes permitted by the aforementioned provision.[101]

4.2 Obstacles to Effective Interoperability

Despite the conferral of a right to reverse engineer, either through decompilation or black-box testing, the exceptions from legal protection offered by the current EU legal system seem far from being considered an effective method to achieve interoperability.[102]

The amount of effort and time required for the decompilation and the strictness of the conditions has led many authors to say that this does not constitute a sufficient mechanism to balance the reward for the author of the computer program with investment in follow-on innovation.[103]

Moreover, TPMs constitute a powerful tool for enforcement of copyright which can be used to prevent extraction of data, and therefore hinder interoperability even where users have in principle a legal right to such interoperability.[104]

---

[101] Knaak, R. / Kur, A. / Hilty, R. (2014), point 36, remarked that in this way the possibility to reverse-engineer software remains largely ineffective.

[102] The European Commission (2013), 13, makes reference to the Microsoft Windows Server Protocols case. Almost a decade of reverse engineering by open-source Samba projects did not manage to yield a fully compatible implementation of the protocols, due to their complexity. The forced licensing of the WSPP by Microsoft was necessary for achieving full interoperability.

[103] Van Rooijen (2010), 86-87; Zingales (2015), 11, which outlines the ambiguity of the language of the decompilation exception, which seems to authorise 'access' and not 'use' of the relevant part of the copyrighted code in the interoperable program.

[104] For a critique of the InfoSoc Directive and the misuse of anti-access software, which can put at risk the freedom to access to and use of works, data and information that could not be covered by copyright, see Ghidini (2010), 114. According to this author 'the problem is not simply that all such provisions are too broad and leave excessive scope for arbitrary conduct. The fact is they lack

4.3 Interoperability in the IoT: Competition-Law Issues in the Standardisation Context

In the light of the above, if intellectual property law were the only set of law to shape the behaviour of firms, these might be encouraged to abstain from standard-setting efforts, with the above-mentioned prejudicial effects for market competition.

This concern drives the intervention of antitrust law, which does not in itself hinder the granting and enjoyment of IPRs, but limits their monopolistic effects to the minimum extent needed to fulfil their essential function of fostering innovation, creativity and trade identity.[105]

European competition law incorporates the idea that where an input is necessary to provide access to an essential infrastructure, its sharing will likely be imposed *ex post,* to the extent that withdrawal of the input prevents actual and potential competitors from bringing about a new product or a technical development. Suffice it to mention the cases in the US and Europe against Microsoft, where the EU Commission held Microsoft liable of abuse of dominant position in the PC operating system market in two ways: by deliberately restricting interoperability between Windows PCs and non-Microsoft work group servers, and by tying its Windows Media Player (WMP) with its Windows operating system.[106] This decision of the Commission was then confirmed by the Court of First Instance of the EU.[107]

As a consequence, limitations to interoperability could result in the Commission finding an abuse by a dominant undertaking, given that this practice could be used as a means to stifle competition.

In other circumstances, the Commission can limit itself to accepting commitments offered by the undertakings concerned, as happened as far back as 1984, when the Commission accepted the proposal from IBM to provide timely interoperability information to its competitor.[108]

---

teeth. The Directive does not provide any effective means to prevent and chastise, with appropriate sanctions and procedures, the application of TPM to non-copyrightable data and information'.

[105] Ghidini (2010), 15.

[106] European Commission, Case No. COMP/C-3/37.792 – Microsoft, 24 March 2004. As remedies the European Commission ordered Microsoft 'within 120 days, to disclose complete and accurate interface documentation which would allow non-Microsoft work group servers to achieve full interoperability with Windows PCs and servers' and 'within 90 days, to offer to PC manufacturers a version of its Windows client PC operating system without WMP'.

[107] GC, Microsoft / Commission, T-201/04, ECLI:EU:T:2007:289. For remarks see Surblytė (2011), 5; Howarth / McMahon (2008); Larouche (2008); Ahlborn / Evans (2009); Kühn / Van Reenen (2009).

[108] See European Commission (1984), para. 94-95.

More recently, the Commission has approved the acquisition of McAfee by Intel subject to a twofold obligation by the latter: (a) to ensure that interoperability and optimisation information will be available to vendors of Endpoint Security Software pursuant to suitable contractual agreements and (b) not to actively engineer or design its microprocessors to degrade the performance of the mentioned device.[109]

Relying on the EU Treaty rule on abuse of dominant position (Article 102 TFEU), the European Court of Justice indicated in *Magill*[110] and *IMS*[111] that IPR holders may be forced to grant other firms a licence for standard-essential patents (SEPs) (cf. *infra sub* para. 6).

This means that manufacturers of standard-compliant products have a right to obtain a licence from holders of patents that are essential to the standard in question, to promote interoperability between devices or networks. The licence is to be granted in exchange for compensation, the level of which should be fair, reasonable and non-discriminatory (FRAND) but actually is a complex question that has often led to disagreements and litigation.[112]

---

[109] European Commission, Case No. COMP/M.5984 – Intel/McAfee, 26 January 2011. The Italian Competition Authority recently dealt with the existence of an alleged exclusionary strategy put in place by Net Service, the company which designed and exclusively operates the technology infrastructure for the management of the Italian civil proceedings (called PCT), against some companies active in the production, distribution and sale of software applications for the PCT. The Authority claimed that Net Service was involved in the late, incomplete or missing communication of the technical specifications needed for the interoperability of the systems, with the aim to hinder competition in the downstream market. The Authority found that the dominant position held by Net service in the upstream market allows it to know, ahead of competitors in the downstream market, the information needed to improve software applications and stressed that, based on this position, Net Service had 'a competitive duty to promptly make available to competitors the same information which it holds'. In order to overcome the existing information gap, Net Service proposed different commitments, which have been accepted by the Authority with its decision of 18 January 2017, available at http://www.agcm.it/concorrenza/concorrenza-delibere/open/41256297003874BD/E22642DE894AFBFCC12580B800544D4F.html.

[110] ECJ, RTE and ITP v Commission, C-241/91 P and C-242/91 P, ECLI:EU:C:1995:98, para. 50. See Vinje (1995), The final world on Magill, Rivista di diritto industriale, I, 239.

[111] ECJ, IMS Health, C-418/01, ECLI:EU:C:2004:257, para. 35 and 52. See Drexl (2004) and Conde Gallego (2006).

[112] Pursuant to the Guidelines, the assessment of whether the licensing terms respect these requirements 'should be based on whether the fees bear a reasonable relationship to the economic value of the IPR', making reference to the test developed by the ECJ, United Brands, C-27/76, ECLI:EU:C:1978:22, despite some commentator deemed this test poorly suited to determine the excessiveness of non-physical constructs, such as intellectual property rights, see Geradin (2009), 329. For different methods which can be adopted to make this assessment see Guidelines, at § 289. In general, the issue of the meaning of the terms 'fair' and 'reasonable' contained in the FRAND promise has absorbed the attention of legal and economic commentators in the last few years. See, e.g., Swanson / Baumol (2005); Geradin / Rato (2007); Mariniello (2011); Carlton / Shampine (2013).

5 Personal Data, Competition and IP Law: Towards a 'Holistic Approach'?

In the light of the above, the research question which this book seeks to explore seem to warrant a positive answer. The new IoT business model, which relies as its fundamental attributes on connectivity, interoperability and information exchange, lends itself easily to a holistic or integrated legal approach.

Indeed, the issue of interoperability between competing devices that has been addressed in this chapter shows well how the needs for protection of consumers and business interests can be best accounted for at the IP/competition law intersection.[113]

European institutions have long been convinced of the case for taking this kind of action.[114] The first important contribution on the complex interface between standardisation, intellectual property and competition law is normally identified with the European Commission's 1992 Communication on Intellectual Property Rights and Standardization,[115] which emphasised the need for European standard-setting organisations (SSO) and members of such organisations to comply with EU competition rules.

Nevertheless, the Commission already recognised the value of interoperability in the current technological landscape within the preamble of Directive 95/47/EC on the use of standards for the transmission of television signals. Therein it stated that 'in the broadcasting of television signals, it is necessary to take steps to adopt a common format for wide-screen transmissions'.[116] This goal was considered instrumental 'to contribute to the proper functioning of the internal market'.

Almost 10 years later, the European Commission launched its first major investigations regarding the compatibility with EU competition law of the licensing conduct of SEP holders, i.e. the US-based technology companies Rambus and Qualcomm, accused to have charged excessive royalties for their patents. No one case concluded with a substantial decision able to set clear principles,[117] so the

[113] The concept of an 'IP/competition law intersection' has been developed by Ghidini (2010), 210, who explains how the systemic distinction between IP law and antitrust law 'should not overshadow a more complex intertwining of relationships and functions between the two' and defines this relationship as 'a tale of two regulations whose goal and basic regulatory principles can't be held to coincide'. For a comprehensive discussion of the complex relationship between IPR and competition law see also Anderman (2001).

[114] Joaquin Almunia, former Competition Commissioner stated 'The lesson we have learned so far from our enforcement in these ICT industries … is that they are highly complex sectors, characterised by the need for interoperability and by potentially strong network effects or risk of lock-in. Often, these are markets where single companies dominate and it is therefore essential to ensure competition on the merits, notably through innovation', see Almunia (2010a), 4.

[115] European Commission (1992).

[116] Ghidini (2015), 437.

[117] European Commission, Case No. COMP/38.636 – Rambus, 9 December 2009. Rambus was preliminarily found to have engaged in a 'patent ambush' by intentionally concealing that it had SEPs, and by subsequently charging royalties for those SEPs that it would not have been able to

Commission decided to provide some guidance, issuing the Guidelines on the applicability of Article 101 TFEU to horizontal cooperation agreements.[118]

The next steps were marked by the Commission's case law, with the decisions that cleared the merger between Google and Motorola Mobility Inc. (MMI), as well as between Microsoft and Nokia,[119] and by the so-called smartphone patent war, in which several major technology companies sought to ban competitors' products from the market on the basis of their SEPs.[120] The Commission's decisions against Samsung[121] and Motorola[122] and the Court of Justice judgment of July 2015[123] in the context of a patent infringement action initiated by Huawei against its Chinese rival ZTE developed a framework outlining the circumstances under which an SEP holder could seek an injunction against a standard implementer to enforce its patents without breaching Article 102 TFEU.[124]

What we have seen during these 10 or 20 years is therefore that any time there is a big step forward in the technology (from before 3G to 4G mobile telecommunica-

---

charge absent its conduct. The Commission adopted an 'Article 9 commitments' decision, whereby it rendered legally binding the worldwide capped on its royalty rates for products compliant with the relevant standards for a period of five years committed by Rambus. Instead in Qualcomm the investigation was closed in advance, see http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_39711.

[118] European Commission (2011). The Guidelines sets the conditions under which such agreements would normally fall outside the scope of Article 101(1): they indicate that when (i) participation in standard-setting is unrestricted and (ii) the procedure for adopting the standard in question is transparent, standardisation agreements which contain no obligation to comply with the standard and provide access to the standard on FRAND terms will normally not restrict competition within the meaning of Article 101(1). Antitrust Guidelines for the Licensing of Intellectual Property were adopted in 1995 also by the U.S. Department of Justice Antitrust Division and the Federal Trade Commission (FTC). On 12 August 2016 a proposal for updating the Guideline was issued but it does not address conducts involving standard essential patents.

[119] European Commission, Case No. COMP/M.6381 – Google / Motorola Mobility, 13 February 2012; European Commission, Case No. COMP/M.7047 – Microsoft/ Nokia, 4 December 2013.

[120] For an overview see Frank (2015), 81.

[121] European Commission, Case No. AT.39939 – Samsung - Enforcement of UMTS standard essential patents, 29 April 2014. The alleged infringement consisted of the seeking of injunctions against a willing licensee, Apple, before the German, Italian, Dutch, UK and French courts, aiming at banning certain Apple products from the market on the basis of several Samsung 3G SEPs which it had committed to license on FRAND terms. Samsung committed not to seek injunctions in Europe on the basis of SEPs for mobile devices for a period of five years against any potential licensee of these SEPs who agrees to accept a specific licensing framework, consisting of a mandatory negotiation period of up to 12 months and if the negotiation fails, third party determination of FRAND terms by either a court, if one party chooses, or arbitration if both parties agree.

[122] European Commission, Case No. AT.39985 – Motorola - Enforcement of GPRS standard essential patents, 29 April 2014. The Commission found an infringement of the EU competition rules in Motorola's seeking and enforcement of injunctions against a willing licensee, Apple, on the basis of one of Motorola's SEPs.

[123] ECJ, Huawei Technologies, C-170/13, ECLI:EU:C:2015:477. For further remarks see Alison (2014).

[124] For a complete chronological analysis of this steps, see Geradin (2017).

tions and the smartphone) there has been a corresponding surge of patent litigation in order to resolve competing patent litigation.

It may be too easy to predict that IoT technologies are going to be next. In this case, the feeling is that the principles established in these cases should be applied even beyond the smartphone industry.[125]

6 The Policy Framework for Regulating Standard-Setting in the EU

Competition law's ability to effectively prevent the emergence of anti-competitive behaviour, such as limitations to interoperability, should not be overestimated. Indeed, if an undertaking is not dominant, there is not much that the Commission could do against refusal to license IPRs, as the right holder just exercises its right to decide whether and under which conditions to license.[126] Furthermore, by the time a competition authority has the grounds to intervene, competition may already be distorted and network effects may make it difficult to restore effective competition. Indeed, competition law continues to be perceived as an ex-post, reactive regime.

Therefore its action, in order to be effective, must be supported and complemented by rapid standard-setting procedures.[127] The European Commission's 2009 Communication already considered the 'necessary standardisation of IoT technologies' as one of the main lines of action to develop. Some steps in this direction were taken in 2013, when the Commission issued its Staff Working Document entitled *Analysis of measures that could lead significant market players in the ICT sector to license interoperability information*.

The Commission dealt with some of the issues outlined in this paper, such as patent, copyright and trade secret protection of the interoperability information. Having noted the state of the law with regard to those three areas, the Commission concluded that non-legislative measures for enhancing interoperability (adopting guidelines to assess the value of interoperability information, developing best practices on the availability of interoperability information or drafting model licences

[125] See Competition Directorate - General of the European Commission (2014), 1.

[126] In the absence of dominance, the Commission may consider the terms and conditions of licence under Article 101(1) TFEU. Therefore, the definition of one or several product and geographic market and the determination of the presence of dominance on such market is a key issue.

[127] This was recognised by Almunia (2010b), 2 which stated that 'a case by case ex-post intervention is not always efficient to deal with structural problems, competition and sector regulation will need to work hand in hand, pursuing the same objectives through complementary means'. In the same sense, Da Coreggio Luciano / Walden (2011), 16 and Posner (2001), 925, according to which 'The real problem lies on the institutional side: the enforcement agencies and the courts do not have adequate technical resources, and do not move fast enough, to cope effectively with a very complex business sector that changes very rapidly'. See also Kester (2016), 217, who considers IoT standards as 'critical to the success and expansion of IoT devices and networks'.

for interoperability[128]) should be preferred to legislative options.[129] It reasoned that these measures would have a more immediate impact and would contribute to fostering 'a culture of licensing and exchange in the spirit of open innovation'.

In 2014, a foresight study by the European Commission Joint Research Centre emphasised the need for anticipating standards requirements and accelerating their development in Europe.[130] In 2015, The Commission and various key IoT players launched a large-scale alliance called AIOTI (Alliance for Internet Of Things Innovation), aimed at assisting the European Commission with the innovation and standardisation policies.[131] The AIOTI structure consists of the Board (Steering Committee) and eleven Working Groups (WGs) corresponding to current prominent areas of development in the field of IoT. One of them is entirely devoted to dealing with 'IoT Standardisation', which implies the mapping of existing IoT standards and gap analysis, as well as strategies and use cases to develop interoperability.[132] In this regard, significant progress has been made with the creation of private organisations with the specific scope of reconciling standards with respect to IoT.[133]

[128] The Commission effectively included into the model agreement for Horizon 2020 optional clauses for interoperability.

[129] The Commission examined two options that could be implemented in relevant legislations to facilitate interoperability. A first measure could be to make licences of patents which cover interoperability information under FRAND terms mandatory. Such a measure would be add to the similar obligation to grant licences of SEPs under FRAND terms already existing in the IPR policies of standardisation bodies.

As an alternative, the Commission also evaluated an interoperability directive based on Article 114 TFEU addressing cases where market players are unwilling to license rights on reasonable terms. This proposal should mirror Directive 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive). Its Article 8(2) provides for connection obligations on undertakings with significant market power in the telecom domain.

Another approach could be to introduce an interoperability exception for patents, mirroring that already existing in the Software Copyright Directive (cf. para. 4.1.2).

[130] European Commission Joint Research Center (2014). Member States are also sponsoring initiatives in this field. For instance, the Italian Industrial National Plan 4.0 for 2017-2020 presents among the measures aimed to support Industry 4.0 developments 'collaboration for the definition of IoT standard communication protocols'.

[131] See https://ec.europa.eu/digital-single-market/alliance-internet-things-innovation-aioti.

[132] See https://ec.europa.eu/digital-single-market/aioti-structure.

[133] For example the AllSeen Alliance, created in December 2013 and chartered by Qualcomm, Cisco, Panasonic and other; the Open Interconnect Consortium (OIC), established in July 2014 by Intel, Samsung, Dell and then joined by Hewlett Packard and Lenovo. Recently a new licensing platform called Avanci has been introduced. Built on the traditional idea of the patent pool, it aims to offer flat-rate licences on FRAND terms for a collection of standard essential wireless patents, with the aim of removing the need to negotiate multiple bilateral licences. For other groups see Kester (2016), 218.

7 Conclusion

In conclusion, the IoT business model is a significant example of how the full range of public rules designed to ensure that markets are competitive must work together. Antitrust, IP law, standard-setting public policies and data protection law (if not also consumer law, which is beyond the scope of this work) only constitute individual tools in the competition policy toolkit.[134] Thus the 'holistic approach' that the 2014 EDPS' Opinion devised in order to attract privacy concerns in merger investigations, could have a significantly larger horizon and could lead to a closer dialogue between regulators to promote growth and innovation as well as consumers' welfare.

Acknowledgements I am very grateful to Prof. Gustavo Ghidini and Prof. Marco Ricolfi for their comments on an earlier draft of this article.

References

Abramson, B. (2008), Are "Online Markets" Real and Relevant? From the Monster-Hotjobs Merger to the Google-Doubleclick Merger, 4 Journal of Competition Law and Economics, 655-662

Ahlborn, C. / Evans, D.S. (2009), The Microsoft Judgment and its implications for Competition Policy Towards Dominant Firms in Europe, 75 Antitrust Law Journal, 887-932

Alison, J. (2014), Standard-essential Patents: FRAND Commitments, Injunctions and the Smarthphone Wars, 10 European Competition Journal, 1-36

Anderman, S.D. (2001), EC Competition Law and Intellectual Property Rights: The Regulation of Innovation, Oxford University Press, 1-392

Aplin, T. (2005), The ECJ elucidates the database right, 2 Intellectual Property Quarterly, 204-221

Balough, C.D. (2011), Privacy Implications of Smart Meters, 86 Chicago Kent Law Review,161–191

Barbry, E. (2012), The Internet of Things, Legal Aspects What Will Change (Everything)…, 87 Communications and Strategies, 83-100

Barker, E. / Harding, I. (2012), Copyright, the ideas/expression dichotomy and harmonization: digging deeper into SAS, 7 Journal of Intellectual Property Law and Practice, 673-679

Brown, I. (2014), Britain's Smart Meter Programme: A Case Study in Privacy by Design, International Review of Law, 28 Computers & Technology, 172-184

Carlton, D. W. / Shampine, A. (2013), An Economic Interpretation of FRAND, 9 Journal of Competition Law and Economics, 531-552

Cavoukian, A. (2013), Privacy by Design: Leadership, Methods, and Results, in: S. Gutwirth / R. Leenes / P. de Hert / Y. Poullet (Eds.), European Data Protection: Coming of Age, Springer, 175-202

Ciani (2017), Property rights model v. contractual approach: How protecting non-personal data in cyberspace?, Diritto del Commercio Internazionale, 4, 831–854

Ciani (2018), Governing Data Trade in Intelligent Environments: A Taxonomy of Possible Regulatory Regimes Between Property and Access Rights, in Chatzigiannakis, I. / Tobe, Y. / Novais, P. / Amft, O. (Eds.), Intelligent Environments, IOS Press, 285–297

[134] Hovenkamp (2008), 104.

Conde Gallego, B. (2006), Die Anwendung des kartellrechtlichen Missbrauchsverbots auf "unerlässliche" Immaterialgüterrechte im Lichte der IMS Health- und Standard-Spundfass-Urteile, 55 Gewerblicher Rechtsschutz und Urheberrecht, Internationaler Teil, 16-28

Cunningham, M. (2014), Next Generation Privacy: The Internet of Things, Data Exhaust, and Reforming Regulation by Risk of Harm, 2 Groningen Journal of International Law, 115-144

Derclaye, E. (2010), Wonderful or Worrisome? The impact of the ECJ ruling in Infopaq on UK Copyright Law, 32 European Intellectual Property Review, 247-251

Drexl, J. (2004), IMS Health and Trinko – Antitrust placebo for consumers instead of sound economics in refusal-to-deal case, International Review of Intellectual Property and Copyright Law, 788-808

Edwards, L. (2016), Privacy, security and data protection in smart cities: a critical EU law perspective, 2 European Data Protection Law Review, 28-58

Ferguson, A.G. (2016), The Internet of Things and the Fourth Amendment of Effects, 104 California Law Review, 805-880

Frank, J.S. (2015), Competition concerns in Multi-Sided Markets in Mobile Communication, in: G. Surblytė (Ed.), Competition on the Internet, 23 MPI Studies on Intellectual Property and Competition Law, Springer, 81-99

Froomkin, M. (2000), The death of privacy, 52 Stanford Law Review, 1461-1543

Garfinkel, S. (2000), Database nation: the death of privacy in the 21st century, O'Reilly Media, 1-388

Geradin, D. (2009), Pricing Abuses by Essential Patent Holders in a Standard-Setting Context: A View from Europe, 76 Antitrust Law Journal, 329-357

Geradin, D. (2017), European Union Competition Law, Intellectual Property law and Standardization, in: J.L. Contreras (Ed.), The Cambridge Handbook of Technical Standardization Law, Cambridge University Press, forthcoming

Geradin, D. / Rato, M. (2007), Can Standard-Setting Lead to Exploitative Abuse? A Dissonant View on Patent Hold-up, Royalty-Stacking and the Meaning of FRAND, 3 European Competition Law Journal, 101-161

Ghidini, G. (1995), Prospettive "protezioniste" nel diritto industriale, Rivista di diritto industriale, 73-98

Ghidini, G. (2006), Intellectual Property and Competition Law: The Innovation Nexus, Edward Elgar, 1-176

Ghidini, G. (2010), Innovation, Competition and Consumer Welfare in Intellectual Property Law, Edward Elgar, 1-304

Ghidini, G. (2015), Profili evolutivi del diritto industriale, Giuffrè, 1-487

Ginsburg, J.C. (1994), Four Reasons and a Paradox: The Manifest Superiority of Copyright over Sui Generis Protection of Computer Software, 94 Columbia Law Review, 2559-2572

Gordon, W.J. (1992), On Owning Information: Intellectual Property and the Restitutionary Impulse, 78 Virginia Law Review, 149-281

Holtzman, D. (2006), Privacy lost: how technology is endangering your privacy, Jossey-Bass, 1-352

Hovenkamp, H. (2008), Innovation and the Domain of Competition Policy, 60 Alabama Law Review, 103-131

Howarth, D. / McMahon, K. (2008), Windows has performed an illegal operation: The Court of First Instance's Judgement in Microsoft v Commission, 29 European Competition Law Review, 117-134

Kester, R. (2016), Demystifying the Internet of Things: industry impact, standardization problems, and legal considerations, 8 Elon Law Review, 205-227

Klitou, D. (2014), Privacy-Invading Technologies and Privacy by Design, Springer, 1-330

Knaak, R. / Kur, A. / Hilty, R. (2014), Comments of the Max Planck Institute for Innovation and Competition of 3 June 2014 on the Proposal of the European Commission for a Directive on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure of 28 November 2013, Com(2013)813 Final, 45 International Review of Intellectual Property and Competition Law (IIC), 953-967

Koops, B.-J. (2014), On Legal Boundaries, Technologies, and Collapsing Dimensions of Privacy, 2 Politica e Società, 247-264

Kühn, K.-U. / Van Reenen, J. (2009), Interoperability and Market Foreclosure in the European Microsoft Case, in: B. Lyons (Ed.), Cases in European Competition Policy: The Economic Analysis, Cambridge University Press, 50-72

Lee, T.B. (2014), Everything's Connected: How Tiny Computers Could Change the Way We Live, Vox (13 August 2014), available at: http://www.vox.com/2014/5/8/5590228/how-tiny-computers-could-change-the-way-we-live.

Lemley, M.A. (1995), Convergence in the Law of Software Copyright, 10 Berkeley Technology Law Journal, 1-34

Leta Jones, M. (2015), Privacy without Screens & the Internet of other People's Things, 51 Idaho Law Review, 639-660

Levin, A. (2007), Big and Little Brother: The Potential Erosion of Workplace Privacy in Canada, 22 Canadian Journal of Law and Society, 197–230

Lim, D. (2014), Standard Essential Patents, Trolls, and the Smartphone Wars: Triangulating the End Game, 119 Penn State Law Review, 1-91

Lindhorst (2011), EuGH: Grafische Benutzeroberfläche genießt keinen Urheberrechtsschutz als Computerprogramm, Gewerblicher Rechtsschutz und Urheberrecht, 61

Maras, M.-H. (2015), Internet of Things: Security and Privacy Implications, 5 International Data Privacy Law, 99-104

Mariniello, M. (2011), Fair, Reasonable and Non-Discriminatory (FRAND) Terms: A Challenge for Competition Authorities, 7 Journal of Competition Law and Economics, 523-541

Marly, J. (2011), Der Urheberrechtsschutz grafischer Benutzeroberflächen von Computerprogrammen, 3 Gewerblicher Rechtsschutz und Urheberrecht, 204-208

Marly, J. (2012), Der Schutzgegenstand des urheberrechtlichen Softwareschutzes, Gewerblicher Rechtsschutz und Urheberrecht, 773-779

Masson, A. (2006), Creation of database or creation of data: crucial choices in the matter of database protection, 17 European Business Law Review, 1063-1073

McDonald, A.M. / Cranor, L.F. (2008), The Cost of Reading Privacy Policies, 4 Journal of Law and Policy for the Information Society, 543-568

Menell, P.S. (1989), An Analysis of the Scope of copyright Protection for Application Programs, 41 Stanford Law Review, 1045-1104

Menell, P.S. (2017), API Copyrightability Bleak House: Unraveling the Oracle v. Google Jurisdiction Mess, Berkeley Technology Law Journal, forthcoming, available at: http://www.law.nyu.edu/sites/default/files/upload_documents/Menell%20-%20API%20Copyrightability%20Bleak%20House.pdf

Miller, A.R. (1993), Copyright Protection for Computer Programs, Databases, and Computer-Generated Works: Is Anything New Since CONTU?, 106 Harvard Law Review, 977-1073

Murphy, M.H. (2015), The Introduction of Smart Meters in Ireland: Privacy Implications and the Role of Privacy by design, 38 Dublin University Law Journal, 191

Nathan, N. (2014), The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google, 40 William Mitchel Review, 854-889

Newton, H. / Moir, A. / Montagnon, R. (2014), CJEU increases burden on manufacturers of games consoles to prove the unlawfulness of devices circumventing technological protection measures and that their TPMs are proportionate, 9 Journal of Intellectual Property Law and Practice, 456-458

Nickless, D. (2012), Functionality of a computer program and programming language cannot be protected by copyright under the Software Directive, 7 Journal of Intellectual Property Law and Practice, 709-711

Nimmer, D. / Bernacchi, R. L. / Frischling, G. N. (1988), A Structured Approach to Analyzing Substantial Similarity of Computer Software in Copyright Infringement Cases, 20 Arizona State Law Journal, 625-656

O'Hara, K. / Shadbolt, N. (2008), The spy in the coffee machine: the end of privacy as we know it, Oneworld publications, 1-257
Onslow, R. / Jamal, I. (2013), Copyright Infringement and Software Emulation: SAS Inc v World Programming Ltd, 35 European Intellectual Property Review, 352-356
Peppet, S.R. (2014), Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security & Consent, 93 Texas Law Review, 85-176
Posner, R.A. (2001), Antitrust in the New Economy, 68 Antitrust L.J., 925-943
Reichman, J.H. (1989), Computer Programs as Applied Scientific Know-How: Implications of Copyright Protection for Commercialized University Research, 42 Vanderbilt Law Review, 639-723
Reichman, J.H. (1993), Beyond the Historical Lines of Demarcation: Competition Law, Intellectual Property Rights, and International Trade After the GATT's Uruguay Round, 20 Brooklyn Journal of International Law, 75-120
Robinson, K.W. (2015), Patent Law Challenges for the Internet of Things, 15 Wake Forest J. of Bus. and Intellectual Property Law, 654-670
Rose, D. (2014), Enchanted Objects: Design, Human Desire and the Internet of Things, Scribner, New York, 1-277
Samuelson, P. (2015), Three Fundamental Flaws in CAFC's *Oracle v. Google* Decision, 37 European Intellectual Property Review, 702-708
Samuelson, P. / Davis, R. / Kapor, M.D. / Reichman, J.H. (1994), A Manifesto Concerning the Legal Protection of Computer Programs, 94 Columbia Law Review, 2308-2431
Samuelson, P. / Vinje, T. / Cornish, W. (2012), Does Copyright Protection Under the EU Software Directive Extend to Computer Program Behaviour, Languages and Interfaces, 34 European Intellectual Property Review, 158-166
Schermer, B. (2010), Privacy and singularity: little ground for optimism?, in: Laurens M., Franken H., van den Herik J., van der Klaauw F., Zwenne G.-J. (eds.), Het binnenste buiten; Liber amicorum ter gelegenheid van het emeritaat van Prof. Dr. Schmidt AHJ, Hoogleraar Recht en Informatica te Leiden, eLaw@Leiden, 305–319
Smith, L. J. (2011), Whether Copyright Protects the Graphic User Interface of a Computer Program, 17 Computer and Telecommunications Law Review, 70-72
Sokol, D.D. / Comerford, R. (2016), Does Antitrust Have A Role to Play in Regulating Big Data?, in: R.D. Blair / D.D. Sokol (Eds.), Cambridge Handbook of Antitrust, Intellectual Property and High Tech, Cambridge University Press, 271-292
Spina, A. (2014), Risk Regulation of Big Data: Has the Time Arrived for a Paradigm Shift in EU Data Protection Law?, 5 European Journal of Risk Regulation, 248–252
Stern, S.M. (2011), Smart-Grid and the Psychology of Environmental Behaviour Change, 86 Chicago Kent Law Review, 139–160
Surblytė, G. (2011), The Refusal to disclose Trade secrets as an Abuse of Market Dominance – Microsoft and Beyond, Stämpfli, Berne, 1-264
Swanson, D.G. / Baumol, W.J. (2005), Reasonable and Nondiscriminatory (RAND) Royalties, Standards Selection, and Control of Market Power, 73 Antitrust Law Journal, 1-58
Terry, N.P. (2016), Will the Internet of Things Disrupt Healthcare?, 19 Vand. J. Ent. & Tech. L., 327-353
Thierer, A. (2015), The Internet of Things and Wearable Technology Addressing Privacy and Security Concerns without Derailing Innovation, 21 Richmond Journal of Law & Technology, 1-118
Van Rooijen, A. (2010), The Software Interface between Copyright and Competition Law: A Legal Analysis of Interoperability in Computer Programs, Kluwer Law, 1-312
Vinje (1995), The final world on Magill, Rivista di diritto industriale, I, 239
Weber, R.H. / Weber, R. (2010), Internet of Things: Legal Perspectives, Springer, 1-135
Weber, R.H. (2015), Internet of Things: Privacy issues revisited, 31 Computer Law & Security Review, 618-627

Whitaker, R. (2000), The end of privacy: how total surveillance is becoming a reality, New Press, New York, 1-195
Willborn, S.L. (2006), Consenting Employees: Workplace Privacy and the Role of Consent, 66 Louisiana Law Review, 975–1008

Additional Sources

Almunia, J. (2010a), New Transatlantic Trends in Competition Policy, 10 June 2010, available at: http://europa.eu/rapid/press-release_SPEECH-10-305_en.htm?locale=en
Almunia, J. (2010b), Competition policy for an open and fair digital economy, 29 October 2010, available at: http://europa.eu/rapid/press-release_SPEECH-10-610_en.htm
Arnold, R. / Hillebrand, A. / Waldburger, M. (2015), Personal Data and Privacy - Final Report - Study for Ofcom, WIK-Consult
Article 29 Working Party (2013), Opinion 03/2013 on purpose limitation, (WP 203), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf
Article 29 Working Party (2014), Opinion 8/2014 on Recent Developments on the Internet of Things, (WP 223), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf
Ashton, K. (2009), That 'Internet of Things' Thing, RFID J., available at: http://www.rfidjournal.com/articles/view?4986
Autorité de la concurrence and Bundeskartellamt (2016), Competition Law and Data, available at: http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf
Berkman Center for Internet & Society (2005), Roadmap for open ICT Ecosystems, available at: http://cyber.law.harvard.edu/publications/2005/The_Roadmap_for_Open_ICT_Ecosystems
Bundeskartellamt (2016), Press Release: Bundeskartellamt initiates proceeding against Facebook on suspicion of having abused its market power by infringing data protection rules, 2 March 2016, available at: https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html;jsessionid=78963AD0F7CEC84B0E7EA553D2C6C201.1_cid387?nn=3591568
Competition Directorate - General of the European Commission (2014), Standard-essential patents, Competition policy brief, 8, available at: http://ec.europa.eu/competition/publications/cpb/2014/008_en.pdf
Da Coreggio Luciano, L. / Walden, I. (2011), Ensuring competition in the clouds: the role of competition law, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1840547
Edwards, E. (2008), Stepping Up to the Plate: The Google-Doubleclick Merger and the Role of the Federal Trade Commission in Protecting Online Data Privacy, available at: http://ssrn.com/abstract=1370734
Edwards, L. / Abel, W. (2014), The Use of Privacy Icons and Standard Contract Terms for Generating Consumer Trust and Confidence in Digital Services, CREATe Working Paper 2014/15, available at: http://www.create.ac.uk/blog/2014/10/31/create-working-paper-201415-the-use-of-privacy-icons-and-standardcontract-terms-for-generating-consumer-trust-and-confidence-in-digital-services/
Eskens, S.J. (2016), Profiling the European Citizen in the Internet of Things: How Will the General Data Protection Regulation Apply to this Form of Personal Data Processing, and How Should It?, available at: http://ssrn.com/abstract=2752010
European Commission (1984), XIV Report on Competition Policy, available at: https://publications.europa.eu/en/publication-detail/-/publication/3c93e6fa-934b-4fb9-b927-dc9fed71ccfe
European Commission (1992), Communication on Intellectual Property Rights and Standardization, COM/1992/445 final

European Commission (2009), Communication on Internet of Things: an action plan for Europe, COM/2009/0278 final, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0278:FIN:EN:PDF

European Commission (2011), Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements, C:2011:011:TOC, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2011:011:FULL&from=EN

European Commission (2012), Press Release: Digital Agenda: Commission consults on rules for wirelessly connected devices – the 'Internet of Things', 12 April 2012, available at: http://europa.eu/rapid/press-release_IP-12-360_en.htm

European Commission (2013), Analysis of measures that could lead significant market players in the ICT sector to license interoperability information, SWD(2013) 209 final, available at: https://ec.europa.eu/digital-single-market/en/news/analysis-measures-could-lead-significant-market-players-ict-sector-license-interoperability

European Commission (2014a), Communication Towards a thriving data-driven economy, COM(2014) 442 final, available at: https://ec.europa.eu/digital-single-market/en/news/communication-data-driven-economy

European Commission (2014b), Study on Definition of a Research and Innovation Policy leveraging Cloud Computing and IoT combination (SMART 2013/0037), available at: https://ec.europa.eu/digital-single-market/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination

European Commission Joint Research Center (2014), How will standards facilitate new production systems in the context of EU innovation and competitiveness in 2025?, available at: https://ec.europa.eu/jrc/sites/jrcsh/files/jrc-foresight-study-web_en.pdf

European Data Protection Supervisor (2014), Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf

European Data Protection Supervisor (2016), The coherent enforcement of fundamental rights in the age of big data, EDPS/2016/15, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2016/EDPS-2016-15-Press_Statement_Coherent_Enforcement_EN.pdf

FTC (2015), Report on Internet of Things: Privacy and Security in a Connected World, available at: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013workshop-entitled-internet-things-privacy/150127iotrpt.pdf

Gasser, U. (2015), Interoperability in the Digital Ecosystem, Berkman Center Research Publication No. 2015-13, available at: https://dash.harvard.edu/handle/1/28552584

Gasser, U. / Palfrey, J. (2007), Breaking down digital barriers. When and How ICT Interoperability Drives Innovation, Berkman Publication Series, available at: http://ssrn.com/abstract=1033226

Geradin, D. / Kuschewsky, M. (2013), Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue, available at: https://ssrn.com/abstract=2216088

Kominers, P. (2012), Interoperability Case Study, Internet of Things (IoT), The Berkman Center for Internet & Society Research, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2046984

Lambrecht, A. / Tucker, C.E. (2015), Can Big Data Protect a Firm from Competition, in: A. Ortiz (Ed.), Internet Competition and regulation of Online Platforms, 155-166, available at: https://www.competitionpolicyinternational.com/wp-content/uploads/2016/05/INTERNET-COMPETITION-LIBRO.pdf

Larouche, P. (2008), The European Microsoft Case at the crossroads of competition policy and innovation, TILEC discussion Paper, available at: http://socrates.berkeley.edu/~scotch/DigitalAntitrust/Larouche.pdf

Lerner, A.V. (2014), The Role of "Big Data" in Online Platform Competition, available at: https://ssrn.com/abstract=2482780

Lexinnova (2014), Internet of Things, Patent Landscape Analysis, available at: http://www.wipo.int/export/sites/www/patentscope/en/programs/patent_landscapes/documents/internet_of_things.pdf

Manning, C. (2016), Challenges Posed by Big Data to European Data Protection Law, available at: http://ssrn.com/abstract=2728624

McKinsey Global Institute (2011), Big data: The next frontier for innovation, competition, and productivity, available at: http://www.mckinsey.com/business-functions/business-technology/our-insights/big-data-the-next-frontier-for-innovation

McKinsey Global Institute (2015), The Internet of Things: Mapping the Value Beyond the Hype, available at: http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world

Noto La Diega, G. / Walden, I. (2016), Contracting for the 'Internet of Things': Looking into the Nest, 7 European Journal of Law and Technology, available at: http://ejlt.org/article/view/450

OECD (2013), Exploring the Economics of Personal Data: a survey of methodologies for measuring monetary value, OECD Digital Economy Papers, No. 220, OECD Publishing, Paris, available at: https://doi.org/10.1787/5k486qtxldmq-en

Porter, M.E. / Heppelmann, J.E. (2014), How Smart, Connected Products Are Transforming Competition, Harvard Business Review, available at: https://hbr.org/2014/11/how-smart-connected-products-are-transforming-competition

Samuelson, P. (2015), Functionality and Expression in Computer Programs: Refining the Tests for Software Copyright Infringement, UC Berkeley Public Law Research Paper No. 2667740, available at: https://ssrn.com/abstract=2667740

See Hahn, R.W. / Singer, H.J. (2008), An Antitrust Analysis of Google's Proposed Acquisition of DoubleClick, AEI-Brookings Joint Center Related Publication No. 07-24, available at: https://ssrn.com/abstract=1016189

Spence, W.C. (2016), Fitbit alleges patent infringement in growing market for fitness tracking devices, IP Watchdog, available at: http://www.ipwatchdog.com/2016/01/06/fitbit-alleges-patent-infringement-fitness-tracking-devices/id=64310/

Urquhart, L. / Rodden, T. (2016), A Legal Turn in Human Computer Interaction? Towards 'Regulation by Design' for the Internet of Things, available at: http://ssrn.com/abstract=2746467

Zingales, N. (2015), Of Coffee Pods, Videogames, and Missed Interoperability: Reflections for EU Governance of the Internet of Things, TILEC Discussion Paper No. 2015-026, available at: https://ssrn.com/abstract=2707570

Part III
Personal Data, Civil Law and Consumer Protection

Proprietary Rights in Digital Data? Normative Perspectives and Principles of Civil Law

Lennart Chrobak

Contents

1 Introduction 254
2 Information: Theoretical Foundations 254
2.1 Classification of Information and Data 254
2.2 Data as Economic Input Factor 256
2.3 Data as Legal Input Factor 256
3 Legal Treatment of (Personal) Data in Different Fields of Civil Law 257
3.1 Inter Vivos 258
3.2 Post Mortem: Inheritance Law 264
4 Interim Conclusions and Outlook 266
References 271

Abstract Owing to its significant value for digital and analog business models, information in the form of (personal) data is considered as the new oil of the twenty-first century. However, digital data not only constitute an important economic input factor, but also affect legal sciences and jurisprudence. The present contribution therefore takes the ongoing developments in the digital society as an opportunity to examine (personal) data from the viewpoint of different fields of civil law and discusses possible legal as well as technological solutions for the future.

Lennart Chrobak, Dr. iur., LL.M. (Maastricht), is a postdoctoral research assistant of Prof. Peter Georg Picht at the University of Zurich.

L. Chrobak (✉)
Law Faculty of the University of Zurich, Zurich, Switzerland
e-mail: lennart.chrobak@rwi.uzh.ch

M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law*, MPI Studies on Intellectual Property and Competition Law 28, https://doi.org/10.1007/978-3-662-57646-5_10

1 Introduction

Owing to its significant value, information has been touted, alternatively, as the new currency or the new oil of the digital era. It is therefore undoubted that, within the past three decades, information, often in the form of digital data, has become one of the most significant economic input factors for online businesses. Not only search engines, social networks or online sellers, but also insurance companies and other 'analog' service providers seek to collect, store and analyze data of natural or legal persons in order improve their services and to develop innovative and personalized products. Disruptive information and communication technologies (ICT), such as big-data analytics, have proved to be one of the driving forces of this process.

In order to scientifically assess information and (personal) data in a comprehensive manner, it is necessary to clearly define and delimit the research subject in question. For this reason, first of all, the quality and influence of information and (personal) data will be looked at from the viewpoint of different scientific disciplines. The relevance of information and (personal) data, namely, is not limited to the economic sphere, but is also increasingly becoming an important legal input factor. However, from the perspective of jurisprudence and legal studies, the legal categorization of information and (personal) data appears to be relatively uncertain so far. Moreover, it is a question of principle as to whether the legal order in its current form is still able to keep pace with the rapid technological change and challenges in relation to digital data.

The present contribution takes the ongoing developments in the digital society as an opportunity to conduct a detailed analysis with regard to the qualification and legal categorization of information and digital data from the perspective of different areas of civil law. Conceptually, it differentiates between legal relationships *inter vivos* and *post mortem*. Thus, in the first step, following the delimitation between absolute and relative rights in civil law jurisdictions, particular reference is made to the areas of property law, intellectual property law and the law of obligations. In a second step, the legal implications of the 'digital estate' are described. On the basis of these findings and looking to the future, an attempt is made to formulate possible responses to the existing problems, considering not only new legal approaches, such as 'virtual property' or 'data portability', but also innovative technological solutions, such as block chain technology.

2 Information: Theoretical Foundations

2.1 Classification of Information and Data

'Information' is a very broad and fuzzy term that cannot be easily grasped or precisely described.[1] Constituting both a prerequisite for and result of interpersonal communication, information, in the sense of an at least temporarily existent

[1] Weber (2003), 20; with regard to the different notions of information cf. Zech (2012), 14 et seq.; Lessig (2001), 23, describes information as the 'content layer' in the communications system.

intellectual product, might fulfill various functions in (digital) society.[2] In order to overcome its abstract character and to assure its transaction capacity, information is regularly represented by means of characters or symbols forming codes that can be 'decrypted' by other individuals.[3] Against this background, data can be described as a particular kind of vessel for or representation of information that can be accessed by means of ICT.[4]

In analogy to *information*, *data* does not constitute a singular object, but should be rather conceived as a collective term comprising different categories of data that have to be analyzed in more detail.[5] First of all, a conceptual distinction between *digital data* and *analog data* needs to be made. While the term *digital data* relates to electronic or magnetic signals that are represented by the numeric characters 0 and 1 ultimately constituting continual series of *bits* and *bytes*,[6] *analog data* does not solely differentiate in a black and white manner between 0 and 1, but is able to gradually adjust, i.e. it could also refer to any intermediate value.[7] Furthermore, depending on the storage locations of the digital data in question, a differentiation between *locally stored data*, which are held on a physical storage medium such as a USB stick, a hard drive or a compact disc, and *online data*, which as a rule are placed in a virtual cloud structure,[8] is necessary. In this regard, incorporeal data always have to be separated conceptually from the corporeal data carrier.[9] For the sake of completeness, 'metadata', i.e. data about user data, and 'derived data', i.e. new data generated through the analysis of user data or metadata, need to be considered.[10]

Personal data, which are subject to the legal framework of data protection, include all kinds of (digital) data that are characterized by the fact that they directly or indirectly refer to an identified or at least identifiable natural or legal person.[11] By contrast, we speak of *factual data* if this personal reference is missing. The present publication primarily focuses on the implications of digital data that are either locally stored or saved in the cloud, without being solely confined to personal data. Information and communication technologies also process data that do not fall within the scope of data-protection legislation.

---

[2] Cf. Zech (2012), 14, who suitably defines information as the 'contrary of uncertainty'. See also v. Weizäcker (1971), 51, who considers information as a third autonomous category to be distinguished from matter and consciousness.

[3] Zech (2012), 24 et seq.

[4] Cf. Eckert (2016a), 246; Hess-Odoni (2004), 1; described as the 'code layer' by Lessig (2001), 23, 111.

[5] Cf. also Hürlimann / Zech (2016), 90; Hess-Odoni (2004), 1.

[6] Weber / Chrobak (2015), 6; Eckert (2016a), 246 et seq.

[7] Weber / Chrobak (2015), 6.

[8] In the context of such online data it has to be noted that though data are uploaded to a cloud structure they are ultimately stored on one or more physical data servers of the respective OSP.

[9] Described as the 'physical layer' by Lessig (2001), 23.

[10] Reed (2015), 148.

[11] Cf. e.g. Article 3 (a) Federal Act on Data Protection (FADP); Eckert (2016a), 247; Hürlimann / Zech (2016), 90 et seq.

2.2 Data as Economic Input Factor

The economic relevance of information and data in the online world is undisputed. Some have even gone so far as to call information 'the oil of the 21st century'.[12] When viewed dispassionately, information and data constitute an important economic resource and input factor for electronic as well as analog businesses. Their services are based in whole or in part on the utilization and commercialization of data.[13] Besides online service providers (OSPs), such as online networks (Facebook, Twitter etc.), search engines (Google) or e-commerce platforms, analog service providers, e.g. in the insurance, health-care[14] or financial-services sector, as well as the field of scientific research, might serve as examples in this respect.[15]

Innovative technology and new data-processing techniques thereby prove to be one of the driving forces for new business models.[16] In this context the phenomenon of big-data analytics arouses particular interest. Big-data analytics allows for the automated collection, storage and analysis of large and unstructured volumes of data originating from a variety of sources, at a high velocity. On the one hand, big-data analytics puts OSPs in a position to optimize their business processes and to provide individualized products and services.[17] On the other hand, it allows a conclusion to be drawn on possible consumer preferences and economic developments in the future.

2.3 Data as Legal Input Factor

The respective legal qualification of information and data, as well as their subsequent legal assignment either to the sphere of a particular legal subject or to the public, not only raises fundamental philosophical questions. It also poses challenges to pre-existing patterns of legal thinking and the doctrinal approaches in civil-law jurisdictions.[18] However, neither the various national legal orders nor the sources of international law directly give an explicit answer to the question of who should be entitled to digital data, in the sense of materialized electro-magnetic signals that are represented by numeric characters, and in which form.[19]

---

[12] Wiebe (2016), 877; critical Hürlimann / Zech (2016), 90.

[13] Monopolkommission (2015), 48.

[14] In the context of e-health data reference can be made to the innovative undertaking Healthbank, which seeks to provide a 'citizen-owned health data exchange platform'; see https://www.healthbank.coop.

[15] Monopolkommission (2015), 49 et seq.

[16] Weber / Chrobak (2016a), 3 et seq.; Monopolkommission (2015), 50 et seq.

[17] Monopolkommission (2015), 48; Eckert (2016a), 245.

[18] Weber / Chrobak (2016b), 5.

[19] Weber / Chrobak (2016b), 5.

In a first step, the general relationship between information and the law should be examined. Conceptually, the law can at the same time be located on a superior and an inferior level in relation to information. On the one hand, information can be the subject matter of legal norms formulating general rules of conduct.[20] On the other hand, the law itself can be considered as information in the aforementioned sense. Owing to this complex functional dependency between the autonomous categories of law and information, it appears questionable whether information can be the subject matter of legal norms constituting information itself. However, due to the fact that information has to be conceived as self-referential, i.e. information might be the subject of other information, there is no reason why 'general' information cannot be the subject matter of legal norms as a 'special' kind of information.[21]

So far, the legal analysis in connection with data has primarily focused on the field of fundamental rights, particularly the right to informational self-determination and the right to be forgotten,[22] as well as the problems caused with regard to data-protection legislation. In terms of legal protection, these fields of law first and foremost confer rights of defense against the state and to a limited extent against private individuals.[23]

However, from a scientific viewpoint, the legal implications of data are not constrained solely to defense rights and especially the different areas of civil law allow for 'positive' legal protection. The legal assignment of tangible as well as intangible legal objects to natural or legal persons by means of exclusive or relative rights[24] deserves closer attention in the general discourse about information and data.

3 Legal Treatment of (Personal) Data in Different Fields of Civil Law

The legal assignment of data within the meaning referred to above can be conducted from the perspective of different areas of civil law. From a structural viewpoint, it seems appropriate to make a general distinction between the legal situation *inter vivos* and *post mortem*. In a first step, following the differentiation between absolute and relative rights in civil-law jurisdictions, the legal assignment of data is examined in accordance with property law, intellectual property law and the law of obligations. In a second step, the legal implications of the 'digital estate' in accordance with inheritance law will be examined.

[20] Druey (1995), 29, 32.

[21] Druey (1995), 32.

[22] Cf. ECJ, Google v Spain, C-131/12, ECLI:EU:C:2014:317.

[23] Cf. Briner (2015), 7.

[24] Cf. Zech (2012), 63, who speaks of reification ('Verdinglichung') in this context.

3.1 Inter Vivos

3.1.1 Property Law

The findings of behavioral economics support the conclusion that individuals tend to ascribe an increased value to objects that they perceive as belonging to them than to things owned by other persons.[25] This phenomenon, generally known as the 'endowment effect', does not only apply to tangible objects, such as movable and immovable assets, but can be transferred to intangible objects, such as ideas, intellectual property or digital data.[26] This effect can even be strengthened if the individual has incurred expenses, such as time or capital, to acquire the object in question.[27] As a logical consequence, every individual will seek to attain an exclusive legal position with regard to his or her data.[28]

In civil-law jurisdictions, the assignment of legal objects to particular legal subjects in general takes place in accordance with the national rules of property law.[29] Owing to the exclusionary nature and *erga omnes* effect of proprietary rights, parties are only allowed to refer to the types and content of property rights laid down by law (*numerus clausus*).[30] Moreover, in accordance with the principle of transparency, rights *in rem* have to refer to a precise object (specificity) and must be recognizable to third parties (publicity).[31]

Whether a right *in rem*, such as ownership, which is the most extensive property right in civil-law jurisdictions,[32] such as Switzerland,[33] Germany[34] or Austria,[35] can be validly established with regard to a specific legal object depends on the respective conditions of the national property law in question. In this respect, Swiss private law, in accordance with the wording of Article 641(1) Swiss Civil Code, presupposes the existence of a *res*. In the absence of a legal definition or exemplification,[36] the term has been substantiated by legal doctrine, according to which only

[25] Reed (2015), 139; Lastowka / Hunter (2004), 36.

[26] Reed (2015), 140; Lastowka / Hunter (2004), 36.

[27] Druey (1995), 99; Reed (2015), 139 et seq.

[28] Cf. Weber / Chrobak (2016b), 6; cf. also Hürlimann / Zech (2016), 92.

[29] Cf. Wiegand (2015), Vor Article 641 et seq. N 5. Since Article 345 TFEU prohibits the European Union from prejudicing the rules in the Member States governing the system of property ownership, no harmonization of the national property laws by means of secondary legislation has taken place so far. Cf. Akkermans / Ramaekers (2010), 292.

[30] Van Erp / Akkermans (2012), 65, 67 et seq. In German legal doctrine a subsequent differentiation between the principles of *Typenzwang* and *Typenfixierung* is made.

[31] Van Erp / Akkermans (2012), 75 et seq.

[32] Van Erp / Akkermans (2012), 213.

[33] Cf. Article 641 ZGB.

[34] Cf. § 903 BGB.

[35] Cf. § 354 ABGB.

[36] Eckert (2016a), 247.

'impersonal, corporeal and autonomous objects available to human control' can be the object of proprietary rights.[37] Following a functional approach, it also depends on the public perception whether an object is subsumed under the notion of *res*.[38] Due to the fact that digital data consist solely of materialized electro-magnetic signals, it however appears questionable whether they comply with the requirement of 'corporeality', which is the key element for the definition of a *res*.[39]

When comparing the legal situation in Switzerland with the neighboring civil-law systems, at first sight, there seems to be an uneven picture. While the rules of German property law in a comparable manner state that, pursuant to § 90 BGB, 'only corporeal objects are things as defined by law', the Austrian legal framework, in contrast, adheres to an extensive notion of *res* as indicated in § 353 ABGB, stating that 'corporeal and incorporeal objects' can be subject to ownership rights.[40] Notwithstanding this broadly formulated definition, only tangible objects are completely covered by the Austrian rules on ownership.[41]

On the basis of these findings, the aforementioned criteria imposed by Swiss property law doctrine will now be applied to the different kind of digital data.[42] With regard to locally stored data saved on private physical data carriers such as a USB stick or a hard drive, it becomes obvious that only the storage device satisfies the requirement of corporeality and is thus subject to the property law regime of Articles 641(1) and 713 Swiss Civil Code, respectively[43]; the digital data themselves are, if at all, only indirectly covered by the exclusive rights of ownership.[44] However, it appears rather questionable that the proprietary rights relating to the data carrier can simply be extended to the locally stored data. Since the exclusionary powers of such a 'derived' proprietary right are constrained to the storage medium and have no *erga omnes* effect against third parties, the individual would attain possession of the data on the medium, in the sense of temporary control, rather than effective ownership.[45] Conversely, control over the data carrier does not necessarily indicate that the possessor is entitled to the locally stored data, too.

If, in contrast, the digital data have been uploaded as online data to a cloud structure, with the effect that they are stored on the data servers of the respective OSP, the incorporeal data become neither directly nor indirectly subject to individual property rights of the user. However, as a result of the increasing synchronization between private end-user devices and cloud servers of OSPs, most digital data (or

[37] Meier-Hayoz (1981), Vor Article 641 N 115; Hürlimann / Zech (2016), 91; Hess-Odoni (2004), 2.

[38] Wiegand (2015), Vor Article 641 et seq. N 6.

[39] Wiegand (2015), Vor Article 641 N 5; Briner (2015), 6; Hürlimann / Zech (2016), 92.

[40] Briner (2015), 8; Kletečka / Koziol / Weber (2014), 103.

[41] Kietaibl (2011) in: Fenyves / Kerschner / Vonkilch / Klang, § 354 N 1, 4; Kletečka / Koziol / Weber (2014), 103.

[42] Cf. para. 2.1.

[43] Hess-Odoni (2004), 2.

[44] Cf. Briner (2015), 6; Hess-Odoni (2004), 2; Reed (2010), 1.

[45] Weber / Chrobak (2015), 5.

their copies) are located on various storage media at the same time and thus a clear assignment to the legal sphere of the individual or a third party is not always easy to make. Furthermore, if so-called big-data analytics is employed, it will become even more complicated to separate the different legal spheres, because the metadata constituting the basis for the analysis are generated by the end user, whereas the derived data are created by the OSP or another third party.[46]

Even though the above elaborations regarding the possible classification of digital data as *res* in the sense of Swiss property law are in compliance with the prevailing opinion in legal doctrine and literature, deviating opinions can be found. Some authors, such as Eckert,[47] take the view that incorporeal data should be considered as so-called *res digitalis*,[48] because they fulfill the requirements of controllability as well as corporeality imposed by Swiss property law.[49] By reference to Article 713 Swiss Civil Code, which makes natural forces that are available to human control subject to ownership rights, he furthermore doubts whether the condition of corporeality has to be interpreted *strictu sensu* and pleads for an extended teleological interpretation of the notion of *res* including digital data.[50]

Although, at first glance, the interpretive approach proposed by Eckert might be convincing due to its reference to the well-established system of property law and its allegedly simple implementation through the legislative amendment of Article 713 Swiss Civil Code,[51] it has to be rejected for different reasons to be elaborated subsequently.[52] Due to the non-rivalrous character, intangible nature and ubiquity of digital data, the attempt to establish proprietary rights with regard to them causes problems with respect to two fundamental principles of property law mentioned above.[53]

On the one hand, considering the principle of specificity, it is not clear in the case of digital data which 'object' the proprietary right exactly covers.[54] A major problem is caused by the fact that it is almost impossible to differentiate between the 'original' and the 'reproduction' of digital data or digital content.[55] For instance, in the case of transfer of ownership, it is not impossible for the transferee to obtain a digital data copy, while the transferor still exercises control over the original version. Accordingly, complex legal disputes about the 'quality' of the digital data in

[46] Cf. Wiebe (2016), 878 et seq.

[47] Eckert (2016a), 247 et seq.

[48] Eckert (2016a), 246 et seq; Eckert (2016b), 265.

[49] Critical Hürlimann / Zech (2016), 91 et seq.

[50] Eckert (2016a), 248; dissenting opinion Nänni (2009), 133 et seq.; see also Kälin (2002), 48, 122, according to whom natural forces in the sense of Article 713 Swiss Civil Code are not considered as *res*, but the rules of property law are applied by analogy to them; Hess-Odoni (2004), 6; cf. also Weber / Chrobak (2015), 23.

[51] Eckert (2016a), 249; Eckert (2016b), 273; dissenting opinion Hess-Odoni (2004), 6.

[52] Same opinion Hürlimann / Zech (2016), 92.

[53] Cf. para. 3.1.1 at the beginning.

[54] Cf. also Wiebe (2016), 883.

[55] Merges (2008), 1247 et seq.

question will inevitably occur in the course of the enforcement of such proprietary rights.

On the other hand, it is doubtful whether there is compliance with the principle of publicity, because rights *in rem* in digital data cannot, at least for the time being, be made effectively recognizable to third parties through either possession or registration.[56] In sum, the system of property law in its current state is not suitable to guarantee the control of digital data by individuals.

An alternative approach, to be discussed in more detail below,[57] could be the creation of a new category of so-called 'virtual property rights'[58] in digital data. Aside from the fact that, at least in civil-law systems, the creation of new rights *in rem* is primarily reserved for the democratic legislature,[59] the implementation of virtual property rights could potentially contravene the strict interpretation of the principle of *numerus clausus*, especially in Germany.

3.1.2 Intellectual Property Law

In a structurally comparable manner to the concept of rights *in rem*, which has been discussed before, intellectual property law might confer absolute and exclusive rights in intangible goods to a specific legal person if the necessary protection requirements are met.[60] For the legal assignment of digital data, the main focus lies not on industrial property rights, but primarily on copyright law and database rights.[61] Additionally, the field of knowledge protection (know-how) has to be taken into account.

First of all, digital data can be considered as *work* within the meaning of Article 2(1) Swiss Copyright Act (CopA) and are subject to copyright law under the condition that they have a certain level of originality (*Gestaltungshöhe*) and individual character.[62] Here a general distinction between computer-aided works and computer-generated works has to be made, because only the former, but not the latter, are protected in terms of copyright law.[63] Accordingly, digital data, such as pictures, music or videos, but also whole blogs or websites, can qualify for protection by copyright law if a 'creative step' in the sense of Article 2(1) CopA is involved.[64]

---

[56] Druey (1995), 104 et seq.; cf. Van Erp / Akkermans (2012), 87; Wiebe (2016), 881; dissenting opinion Eckert (2016b), 265 et seq.

[57] Cf. para. 4.

[58] For a general overview cf. Fairfield (2005), 1047 et seq.

[59] Van Erp / Akkermans (2012), 67.

[60] Troller (2005), 16.

[61] Cf. Reed (2015), 141; Hürlimann / Zech (2016), 91.

[62] Troller (2005), 129, 131; Cherpillod (2012), Article 2 CopA N 10; Hürlimann / Zech (2016), 91; with regard to common-law jurisdictions cf. Reed (2010), 10.

[63] Weber / Chrobak (2015), 6 et seq.

[64] Cf. Eckert (2016b), 273; Hürlimann / Zech (2016), 91; Wiebe (2016), 879.

Whether the data in question are locally stored or situated on the servers of third parties is irrelevant in this case.

Moreover, in the context of digital data, computer programs, as a particular kind of software, have to be considered.[65] According to Article 2(3) CopA, computer programs, including *inter alia* online role-playing games or virtual environments, likewise qualify as works in the copyright sense.[66] In this regard, a differentiation is necessary. Article 2(3) CopA only covers digital data bearing program instructions and forming the basis of such environments; except when otherwise stipulated, all other kinds of digital assets, such as valuable avatars or virtual land and chattels, that have been created by the users, are, if at all, protected as audiovisual works in the sense of Article 2(2)(g) CopA. In summary, copyright law only selectively confers intellectual property rights with regard to digital data to end users generating the latter.[67]

Secondly, the legal framework for databases, in the sense of systematic collections of independent works, data or other materials,[68] could be of interest for the legal allocation of digital data. However, in contrast to the European Union, which introduced a *sui generis* right for the protection of databases by means of Article 7(1) Directive 96/6/EC,[69] there is no specific protection of databases under Swiss copyright law.[70] If the conditions of Article 4(2) CopA are fulfilled, structured data collections can be recognized as collected works.[71]

Lastly, in the present context, know-how as a particular manifestation of manufacturing and trade secrets,[72] which in Switzerland are primarily protected under Article 4(c) and Article 6 Unfair Competition Act (UCA),[73] draws interest.[74] The term 'know-how' here refers to both secret and public information which are not (yet) protected by intellectual property law and can be used for commercial purposes, such as the production of goods or the performance of services.[75] On the one hand, know-how might have corporeal manifestations, such as technical reports, formulas and engineering plans, as well as balance sheets, customer and supplier databases or other business information.[76] Since the corporeal manifestations of know-how can, on the other hand, be equally expressed by means of incorporeal

[65] Troller (2005), 22 et seq., 153; Weber / Chrobak (2015), 7.

[66] Cherpillod (2012), Article 2 CopA N 65.

[67] Weber / Chrobak (2015), 8; cf. Reed (2015), 142.

[68] Cf. Article 1 (2) Directive 96/6/EC.

[69] Wiebe (2016), 879.

[70] Reed (2015), 142; Weber / Chrobak (2016b), 11; Hürlimann / Zech (2016), 92.

[71] Weber / Chrobak (2016b), 11.

[72] Cf. Wiebe (2016), 879 et seq.

[73] Cf. also Article 162 Swiss Criminal Code; Mathys (2008), 92 et seq.; Druey (1995), 374; cf. Eckert (2016a), 245 Fn. 5.

[74] Cf. also Article 39(2) TRIPS; cf. Reed (2015), 143 et seq.

[75] Schlosser (1998), 269 et seq.; Ann (2010), in: Ann / Loschelder / Grosch, 5; Dorner (2013), 11 et seq., 24; Druey (1995), 366 et seq.

[76] Dorner (2013), 44; slightly deviating Schlosser (1998), 270.

data,[77] know-how can be considered as a particular subtype of digital data for present purposes.[78] However, due to the limited scope of the current Swiss legal framework, which only applies to secret information with commercial value, in many cases there will be no effective legal protection of digital data as know-how in this sense.[79]

3.1.3 Law of Obligations

If digital data are not subject to the exclusive legal positions provided by property law or intellectual property law, the legal allocation will take place in accordance with the law of obligations, which serves as a kind of legal default mechanism. Contract law only confers relative rights, i.e. the legal effects derived from contracts are limited to the contractual parties and do not take effect *erga omnes*.[80] Hence, contract law is well suited to fulfill these allocation tasks, since it applies to both corporeal and incorporeal objects, including intangible data.[81]

In theory, the parties are able to freely negotiate the individual entitlement to digital data in accordance with the general principle of freedom of contract. However, in practice, the distribution of rights and obligations is mostly governed by preformulated contractual terms,[82] which are imposed on the users by the OSP, who regularly has a stronger negotiation position.[83] Accordingly, the extent to which the user becomes entitled to his or her data depends on the approach followed by the respective OSP.[84]

While some OSPs either, at least purportedly, grant comprehensive rights to the platform users or disregard the issue of 'information ownership',[85] other OSPs reserve the right to make more or less extensive use of all or particular digital data that are generated by the users.[86] Such 'licenses' can thereby refer to digital user data that may or may not be subject to intellectual property rights.[87] A more moderate

[77] Cf. Dorner (2013), 45, who considers electronic data processing as one of the incorporeal manifestations (*unkörperliche Erscheinungsformen*) of know-how.

[78] Cf. Wiebe (2016), 880.

[79] Mathys (2008), 95; cf. Dorner (2013), 146 et seq., 163 et seq. and Wiebe (2016), 880, with regard to the legal situation in Germany and the EU.

[80] Cf. Dorner (2013), 117.

[81] Cf. Hess-Odoni (2004), 3.

[82] In practice often denoted as 'Terms and Conditions' or 'End User License Agreements'.

[83] Reed (2015), 151; Szulewski (2015), 3 et seq.

[84] Reed (2015), 151; cf. also Szulewski (2015), 7 et seq.

[85] Reed (2015), 143 with further examples; Brucker-Kley / Keller / Kurtz / Pärli / Schweizer / Studer (2013), 14 et seq.; Weber / Chrobak (2015), 10.

[86] Fairfield (2005), 1082; Lastowka / Hunter (2004), 50; Weber / Chrobak (2015), 10.

[87] Reed (2015), 143, 151 et seq. If intellectual property or know-how is the subject matter of the contract with the OSP, the distinction can be made between *echte Lizenzverträge* and *unechte Lizenzverträge*; cf. Dorner (2013), 83 et seq. with further evidence; cf. Schlosser (1998), 270 et seq.

example to be mentioned in this respect is Dropbox,[88] which only uses a restricted license that allows the use of the data necessary for the provision of its services. In contrast, Google[89] requires a broader license allowing it to utilize digital content of its users not only for the operation and improvement of its existing services, but also to develop new ones.[90] Even more comprehensively formulated is the so-called IP license employed by Facebook,[91] because it permits almost any kind of use of user data.[92]

In the light of the analysis of the different practical examples made above, the current legal situation cannot be considered as satisfactory.[93] The entitlement of the user to his or her digital data differs considerably and primarily depends on the content of the contractual terms of the respective OSP, which often turn out to be imbalanced and vaguely formulated.

3.2 Post Mortem: Inheritance Law

The legal allocation of digital data is not a mere *inter vivos* issue. Increasingly, attention is drawn to the legal treatment of the 'digital estate'[94] of natural persons in terms of inheritance law.[95] What will happen to my valuable World of Warcraft avatar or my properties in Second Life if I pass away? Who will be allowed to read my Facebook messages? And will my Instagram pictures, YouTube videos or Bitcoins be immediately transferred to my heirs, or do I need to take my own precautions?[96] These are a few of the question that will be examined below in further detail.

In accordance with the general rule in Article 560(1) Swiss Civil Code, on the death of the deceased, the estate in its entirety vests by operation of law in the heirs (universal succession).[97] By way of example, Article 560(2) Swiss Civil Code furthermore states that not only claims, rights of ownership, limited rights *in rem* and rights of possession, but also personal debts of the deceased are automatically transferred to the heirs. Whether digital data qualify as an 'estate' in the sense of

[88] Cf. Dropbox 'Terms of Service', available at: https://www.dropbox.com/privacy#terms.

[89] Cf. Google 'Terms of Service', available at: https://www.google.com/policies/terms/.

[90] Reed (2015), 151 et seq.

[91] Cf. Facebook 'Terms of service', available at: https://www.facebook.com/terms.

[92] Reed (2015), 152.

[93] With the same result Reed (2015), 152.

[94] For a possible definition of the term cf. Deutscher Anwaltverein (2013), 93.

[95] For an overview cf. Weber / Chrobak (2015), 1 et seq. and Künzle (2015), 39 et seq.; with regard to the legal situation in Germany cf. Herzog (2013), 3745 et seq.

[96] For more detailed consideration regarding digital estate planning cf. Künzle (2015), 48 et seq., Szulewski (2015), 14 et seq. and Weber / Chrobak (2015), 17 et seq.

[97] While in German inheritance law the principle of universal succession likewise applies pursuant to § 1922 BGB, Austrian heirs assume the legal position of the deceased by means of devolution (*Einantwortung*) in accordance with § 797 ABGB.

Article 560(1) Swiss Civil Code is not yet comprehensively established.[98] In this respect, particular attention has to be paid to the fact that not the estate objects, but the legal rights of the deceased in relation to them are bequeathed.[99] On the basis of these findings, the close connection between the legal situation *inter vivos* and *post mortem* becomes apparent: as long as the legal entitlement of the deceased is not sufficiently clear, precise statements about the acquisition of the digital estate by the heirs are very difficult to make.[100]

In analogy to the observations made above,[101] three different kinds of digital data constituting the digital estate have to be distinguished. Since in the case of locally stored data the data carrier is directly subject to the proprietary rights referred to in Article 560(2) Swiss Civil Code, the heirs acquire indirect 'ownership' in the digital data derived from and limited to the storage medium. Accordingly, competing entitlements to digital data are not ruled out from the outset.[102] However, assuming that digital data should be separately inheritable from the data carrier would not prove to be feasible in practice. As an example, one could think of a wearable device, such as a smart watch, being bequeathed to a close relative of the deceased, whereas the digital (health) data stored on the smart watch would be bequeathed to a scientific institution for research purposes.

In the case of online data, the legal situation differs depending on whether intellectual property law applies. Under the prerequisite that the digital assets in question, such as virtual avatars or creative digital photographs and videos, show a certain level of originality and individuality in accordance with Article 2(1) CopA, the copyright of the deceased in the digital data may be bequeathed to his or her heirs pursuant to Article 16(1) CopA unless otherwise agreed.[103] If the online data in question are neither indirectly nor directly subjected to the regimes of property law or intellectual property law, respectively, the law of obligations determines the inheritability of data. According to Article 560(2) Swiss Civil Code, the deceased's claims pass to the heirs unless otherwise agreed. Thus, the inheritance of online data, e.g. relating to an online account, indirectly results from the fact that the heirs as legal successors are able to continue the deceased's contractual relationship with the OPS.[104]

Notwithstanding the restrictive approach followed by many terms of service, excluding a succession to the contract between the OSP and the deceased,[105] positive

---

[98] In the affirmative Künzle (2015), 39 et seq.; with regard to Germany cf. Scherrer (2014), § 1 N 30 and Deutscher Anwaltverein (2013), 5.

[99] Herzog (2013), 3747; cf. also Breitschmid / Eitel / Fankhauser / Geiser / Rumo-Jungo (2012), 185.

[100] Cf. Weber / Chrobak (2015), 13.

[101] Cf. para. 3.1.1.

[102] Cf. Weber / Chrobak (2015), 13. For instance, it is possible for identical copies of the data in question to have been generated on foreign cloud servers in the course of synchronization.

[103] Weber / Chrobak (2015), 14 et seq.

[104] Weber / Chrobak (2015), 15; cf. Szulewski (2015), 5.

[105] Cf. Szulewski (2015), 12 et seq. with regard to Yahoo; cf. also Bruckner-Kley / Keller / Kurtz / Pärli / Schweizer / Studer (2013), 14 et seq.; cf. also Kutscher (2015), 101.

self-regulatory initiatives of major OSPs regarding the digital estate can be identified.[106] Aiming to provide for a comprehensive tool for the *post mortem* management of digital data, Google implemented a so-called inactive account manager, which allows the possibility to decide, in a first step, who should receive access to the Google account(s) of the user and, in a second step, which information and data should be made available.[107] In a comparable manner, Facebook allows for the determination of a so-called 'legacy contact', i.e. a trusted person, such as a family member or a close friend, who is asked to take care of the Facebook account if something happens to the account owner in the future.[108] However, the rights of the legacy contact are limited and he or she cannot, *inter alia*, access the account, read messages or change posts.[109]

In the meantime, at least as regards Germany, a certain degree of legal certainty has been created by jurisprudence. The District Court of Berlin issued the first judgment regarding a digital estate and found that all rights under an online contract, such as in the present case with Facebook, are completely inheritable in accordance with § 1922 BGB and that granting access to these data to the heirs is also in compliance with data-protection legislation.[110] However, looking at the pan-European context, legislative actions comparable to the Fiduciary Access to Digital Assets Act issued in the United States of America should also be considered.[111]

4 Interim Conclusions and Outlook

The legal assignment of data to a particular legal subject is a recurring principal theme, and is of vital importance for different fields of civil law that have been elaborated above. Answering this primary question forms the basis for dealing with subsequent data-related issues, such as the trade or transfer of data *inter vivos* and *post mortem*.

The analyzed fields of civil law treat digital data differently. Owing to the strict interpretation of the fundamental principles of property law by legal doctrine, such as the principle of *numerus clausus*, specificity or publicity, and the requirements for protection in terms of intellectual property law, digital data are in most cases subject to the law of obligations. However, the existing imbalance of negotiating power allows OSPs to unilaterally adapt the general terms and conditions to their advantage. The abovementioned practical examples illustrate the inequitable allocation of rights and duties between the contracting parties. Moreover, the legal

[106] Cf. Weber / Chrobak (2016b), 8.

[107] Cf. https://support.google.com/accounts/answer/3036546?hl=en; Szulewski (2015), 10 et seq.

[108] Alternatively, the user can stipulate that the account be permanently deleted; cf. also Szulewski (2015), 7 et seq.

[109] Cf. https://www.facebook.com/help/1568013990080948.

[110] LG Berlin, judgment of 17 December 2015 – 20 O 172/15.

[111] Cf. Szulewski (2015), 15 et seq.

implications of digital data are not limited to the *inter vivos* sphere. Equally, the question can be raised how the law should treat the digital assets of a particular person *post mortem.* The points considered here regarding the digital estate thereby illustrate the existing legal uncertainty, which is compensated to a certain extent by means of voluntary self-regulation of the OSPs.

In the light of the considerations set out above, the legal qualification and assignment of data is not always sufficiently clear. To a certain extent, digital data elude the traditional thought patterns and classification of legal science. As a consequence, loopholes in the protection of the right of individuals are likely. Nevertheless, due to the various cross-references between these structurally separate fields of law, in a long-term perspective a more holistic approach towards the legal treatment and allocation of data will be needed. The aim should be the interdisciplinary development of a new kind of legal framework or network structure comprising relevant legal disciplines, such as civil law, data protection law, intellectual property law or competition law.[112]

Strategic thoughts for the attainment of this goal should not be constrained to the legal perspective, but also need to be seen in the light of the rapid developments in the area of ICT. Thus, in the following, different approaches related to the fields of law and technology will be examined in more detail.

In the legal doctrine of continental European as well as Anglo-American systems, the creation of so-called virtual property rights, in the sense of exclusive rights in digital data, computer code and other virtual assets, such as URLs, email and other online accounts or (parts of) virtual environments,[113] has already been discussed for a while.[114] However, until now, the introduction of such a new category of rights was limited to mere theoretical considerations. This holds true not only for civil-law jurisdictions, such as Switzerland, Germany or Austria, where fundamental conflicts with the principle of *numerus clausus* would occur, but also applies to common-law countries, such as the United States of America.[115]

In contrast, representatives of the Asian legal family take more flexible approaches towards data. While Chinese courts have already acknowledged individual rights in virtual property, e.g. by invoking the principles of contract law (or criminal law),[116] Taiwan has even issued a regulation guaranteeing virtual objects to be effectively protected by means of property law and criminal law.[117] Less successful attempts have been observed in South Korea.[118]

Meanwhile, by means of secondary legislation, the European legislature has reacted to the ongoing discourse about the effective control of data by individuals.

---

[112] Cf. also Weber / Chrobak (2016a), 6.

[113] Cf. Fairfield (2005), 1055 et seq.; Lastowka / Hunter (2004), 30 et seq.

[114] For a general overview cf. Fairfield (2005), 1049 et seq., Purtova (2009), 508 et seq. with further references and Lastowka / Hunter (2004), 29 et seq.

[115] Fairfield (2005), 1063.

[116] Fairfield (2005), 1084 with further references; cf. also Weber / Chrobak (2015), 22.

[117] Fairfield (2005), 1086 et seq.; cf. also Weber / Chrobak (2015), 22.

[118] Fairfield (2005), 1088 et seq.

Though solely applying to personal data, Article 20 of the European General Data Protection Regulation provides for a general 'right to data portability', which should enable the affected individual to transfer his or her data from the platform of one OSP to the platform of another OSP.[119] Notwithstanding the revolutionary character of the idea underlying the concept of 'data portability', seeking to enable the individual to make effective dispositions about his or her data, a lot of open questions have to be answered and several problems still need to be overcome.

First of all, from a functional viewpoint, it is not sufficiently clear whether the right to data portability obliges the OSP to hand over the 'original' data or merely a copy of them. Secondly, in order to allow for the transfer of personal data from one OSP to another, the question of the technological interoperability between the different platforms needs to be resolved. Lastly, the scope of application of Article 20 General Data Protection Regulation is limited to 'personal data',[120] i.e. all other kind of data are not subject to the protection granted by the prospective European legal framework.

As indicated above, possible approaches to the allocation of digital data should also focus on the latest technological developments. A more comprehensive and technologically based solution could be provided by so-called blockchain technology**,** whose advantages for the improvement of financial services and corporate governance are already being discussed.[121]

The term 'blockchain' denotes a private or public peer-to-peer network that serves a decentralized digital ledger for different kinds of (data) transactions made within the network.[122] Using encryption algorithms ('hashing'), the ongoing sequences of these transactions, forming a block, are then chained to the previous block of transaction in order to provide for the immutability of the ledger. Since the content, parties and data of each transaction being made are recorded and verified by every single node of the network, third parties serving as intermediaries and/or central registration authorities become obsolete.[123] Hence, unilateral changes of one transaction become almost impossible, because it would presuppose the alteration of all subsequent blocks in the chain.[124]

Blockchain technology constitutes the technological foundation for holding ownership rights and other entitlements, such as in the digital currency 'Bitcoin', company shares or voting rights, in a single digital wallet. However, since it is for the users to decide what the individually identifiable and programmable units of one

[119] Hürlimann / Zech (2016), 94.

[120] For the definition of 'personal data' see above, para. 2.1.

[121] For an overview cf. Yermeck (2015), 1 et seq.; Schroeder (2015) 1 et seq.

[122] Yermeck (2015), 5; Schroeder (2015), 6; cf. http://www.pwc.com/us/en/technology-forecast/blockchain/definition.html; Roon (2016), 359 et seq.

[123] Roon (2016), 360; Yermeck (2015), 4 et seq.; Schroeder (2015), 6; cf. http://www.pwc.com/us/en/technology-forecast/blockchain/definition.html. In the meantime, the recording functions are primarily fulfilled by so-called miners: well-financed companies that dispose of the necessary computing resources to maintain the ledger of the block chain.

[124] Yermeck (2015), 5; Roon (2016), 360 et seq.

Bitcoin represents,[125] theoretically, other kinds of digital assets, such as an avatar in virtual worlds, or valuable data packages, could equally be part of the virtual wallet.[126]

Blockchain technology proves to be an interesting innovation, because it could, *inter alia*, overcome different (legal) problems with regard to the allocation and control of digital data described above. As an illustrative example, reference can be made to the potential conflict with basic property law principles. First of all, by means of the blockchain, the digital data or assets over which control should be exercised can be clearly specified; the principle of specificity would be satisfied. Secondly, reference to blockchain technology for the allocation of digital data would be in compliance with the principle of publicity. Blockchains not only allow the verification of the genuine entitlement of a natural or legal person to specific packages of digital data, but they could also serve as a kind of public register, making subsequent transfers of 'data ownership' to another party recognizable to third parties, who can rely on the (public) recording function of the peer-to-peer network technology.[127] Thus, blockchain could serve as a technological basis for the trade of data. The advantages of blockchain set out above are not limited to the *inter vivos* sphere, but could also apply to the digital estate of a natural person and serve as a valuable complement to the existing self-regulatory initiative of OSPs like Google or Facebook.

The aforementioned legal and technological approaches, aiming at the effective allocation of information and data, reveal a fundamental conflict of goals between the legal spheres of the individual and the public.[128] Exclusive (legal) positions always presuppose that the legal object in question is withdrawn from the free disposition of the public. In the present case, severe restrictions of the free flow of information and data, constituting one of the cornerstones of the Internet, are likely to occur. The recognition of legal rights in incorporeal objects therefore always requires an explicit justification.[129] As a logical consequence, a 'legal threshold' (*Eingriffsschwelle*) needs to be defined, determining the conditions under which data, in the sense of non-rivalrous goods, can be made subject to the establishment of individual legal positions. Without the implementation of such a primary 'filter' to delimit the legal sphere of the individual and the public, the attempt of a regulatory structure and allocation of data cannot be conducted.

As a structural starting point, one should not focus on the 'location' of the data in question, i.e. whether they are stored on private data carriers or third-party servers. The decisive criterion has to be the content and/or value of the digital data that can be ascribed to or that has been generated by a particular person.[130] As soon as

[125] Yermeck (2015), 7; cf. Roon (2016), 361 et seq.

[126] Roon (2016), 361, legitimately emphasizes the high costs caused by the storage process.

[127] Cf. Yermeck (2015), 1; cf. Roon (2016), 362.

[128] Cf. also Hürlimann / Zech (2016), 92 et seq.

[129] Cf. Dorner (2013), 141.

[130] Cf. also Hürlimann / Zech (2016), 94.

the respective data might create economic value, i.e. if identifiable (packages of) data can be monetarized by third parties, an extraction from the legal sphere of the public and an assignment to a specific legal subject could be envisaged. Broadly speaking, if digital data are considered as the new oil of the twenty-first century, why are they not treated by law in a suitable manner?[131]

The definition of general criteria for the distinction between individual data and data in the public domain appears to be complicated and it will be essential to take into account the specific circumstance of the respective case. Furthermore, (legal) control over digital data presupposes transparency, i.e. the users need to know when, where and by whom their data have been collected, processed and disseminated.[132] In addition, the follow-up issue of 'digital identity' in the sense of effective identification methods of natural and legal persons in digital environments will have to be dealt with, too.[133]

Since digital data as a new kind of legal object are not easily accessible by the traditional structuring approaches of the legal sciences, an adapted interpretation of classical concepts of legal entitlements is required in the digital context. In conformity with a general tendency in legal doctrine and policy, the transformation as well as the conception of legal rights in digital data, which currently resemble relative rights on a contractual basis, does not necessarily have to take place in the sense of an absolute right, such as civil-law ownership, conveying the ability to exclude any third person; 'data ownership' could rather be adopted in a form that essentially provides protection against unjustified exploitation and ensures compensation in case of infringements.[134]

The legal position of the 'data owner' could *inter alia* feature elements of liability rights or of (compulsory) licensing of intangible goods, such as know-how or intellectual property, without being dogmatically limited to those fields of law. The evolved understanding of the genuine idea of 'mine' and 'yours' would acknowledge that there are also shades of grey in the digital world, e.g. in the context of metadata and derived data. In order to ensure the correct accounting of data utilization by third parties, reference could be made to blockchain technology, which allows for the unequivocal allocation of digital data to a particular person. Against the background of the foregoing considerations, it will be interesting to discover which approach will be taken by the European Commission in the course of the 'Digital Single Market Strategy' and, even more recently, the 'European Free Flow of Data Initiative'.[135]

[131] In the same vein Briner (2015), 7 et seq.

[132] Reed (2015), 153.

[133] Cf. Roon (2016), 362.

[134] Cf. Dorner (2013), 119 et seq. with regard to the concept of reification ('Verdinglichung').

[135] Cf. also Wiebe (2016), 877 et seq.

References

Akkermans, B / Ramaekers, E. (2010), Article 345 TFEU (ex Article 295 EC), Its Meanings and Interpretations, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1436478

Ann, / Loschelder, / Grosch, (2010), Praxishandbuch Know-How-Schutz, Heymann (cited: Author in: Ann / Loschelder / Grosch)

Breitschmid, P. / Eitel, P. / Fankhauser, R. / Geiser, T. / Rumo-Jungo, A. (2012), Erbrecht, 2nd ed., Schulthess Verlag

Briner, R.G. (2015), Big Data und Sachenrecht, Jusletter IT of 21 May 2015, available at: http://jusletter-it.weblaw.ch/issues/2015/21-Mai-2015/big-data-und-sachenr_cb093cbe37.html__ONCE

Bruckner-Kley, E. / Keller, T. / Kurtz, L. / Pärli, K. / Schweizer, M. / Studer, M. (2013), Sterben und Erben in der digitalen Welt – Von der Tabuisierung zur Sensibilisierung, vdf Hochschulverlag AG

Cherpillod, I. (2012), in: B.K. Müller / R. Oertli (Eds.), Handkommentar Urheberrechtsgesetz, Stämpfli Verlag AG

Deutscher Anwaltverein (2013), Stellungnahme zum digitalen Nachlass, available at: https://anwaltverein.de/files/anwaltverein.de/downloads/newsroom/stellungnahmen/2013/SN-DAV34-13.pdf

Dorner, M.H. (2013), Know-how-Schutz im Umbruch: Rechtsdogmatische und informationsökonomische Überlegungen, Diss. München 2002, Carl Heymanns Verlag

Druey, J.N. (1995), Information als Gegenstand des Rechts, Schulthess Verlag

Eckert, M. (2016a), Digitale Daten als Wirtschaftsgut: digitale Daten als Sache, 112 Schweizerische Juristen-Zeitung 245

Eckert, M. (2016b), Digitale Daten als Wirtschaftsgut: Besitz und Eigentum an digitalen Daten, 112 Schweizerische Juristen-Zeitung 265

Van Erp, S. / Akkermans, B. (2012), Cases, Materials and Text on Property Law, Hart Publishing

Fairfield, J.A.T. (2005), Virtual Property, 85 Boston University Law Review 1047

Fenyves, A. / Kerschner, F. / Vonkilch, A. / Klang, H. (Eds.) (2011), §§ 353 bis 379 ABGB, 3rd ed., Verlag Österreich (cited: Author in: Fenyves / Kerschner / Vonkilch / Klang)

Herzog, S. (2013), Der digitale Nachlass – ein bisher kaum gesehenes und häufig missverstandenes Problem, 52 Neue Juristische Wochenschrift 3745

Hess-Odoni, U. (2004), Die Herrschaftsrechte an Daten, Jusletter of 17 May 2004, available at: http://jusletter.weblaw.ch/juslissues/2004/277/_2889.html

Honsell, H. / Vogt, N.P. / Geiser, T. (Eds.) (2015?), Basler Kommentar Zivilgesetzbuch II, 5th ed., Helbing & Lichtenhahn (cited: BSK ZGB-Author)

Hürlimann, D. / Zech, H. (2016), Rechte an Daten, sui-generis 2016, 89

Kälin, D. (2002), Der Sachbegriff im schweizerischen ZGB, Diss. Zürich 2002, Schulthesss Verlag

Kletečka, A. / Koziol, H. / Weber, R. (2014), Grundriss des bürgerlichen Rechts, Band 1, Allgemeiner Teil, Sachenrecht, Familienrecht, 14th ed., Manz

Künzle, H.R. (2015), Der digitale Nachlass nach schweizerischem Recht, successio 2015, 1, 39

Kutscher, A. (2015), Der digitale Nachlass, Diss. Göttingen 2015, V & tR unipress

Lastowka, F.G. / Hunter, D. (2004), The Laws of the Virtual Worlds, 1 California Law Review 3

Lessig, L. (2001), The future of ideas: The fate of the commons in a connected world, 1st ed., Random House

Mathys, R. (2008), Know-how-Transfer, -Erhaltung und -Sicherung beim ICT-Outsourcing, in: O. Arter / L. Morscher (Eds.), ICT-Verträge – Outsourcing, Stämpfli Verlag AG

Meier-Hayoz, A. (1981), Kommentar zum Schweizerischen Privatrecht (Berner Kommentar), Das Sachenrecht, Bd. 4, 1. Abteilung, 1. Teilband, Das Eigentum, Article 641-654, 5th ed., Stämpfli Verlag AG

Merges, R.P. (2008), The concept of property in the digital era, 4 Houston Law Review 1240

Monopolkommission (2015), Sondergutachten 68, Wettbewerbspolitik: Herausforderung digitale Märkte, Nomos Verlag

Nänni, M. (2009), Märkte virtueller Welten, Diss. Zürich 2009, Schulthess Verlag
Purtova, N. (2009), Property rights in personal data: Learning from the American discourse, 25 Computer Law & Security Review 507
Reed, C. (2015), Information in the cloud: ownership, control and accountability, in: A.S.Y. Cheung / R.H. Weber (Eds.), Privacy and Legal Issues in Cloud Computing, Edward Elger Publishing
Reed, C. (2010), Information 'Ownership' in the Cloud, Queen Mary University of London, School of Law, Legal Studies Research Paper No. 45/2010, available at: http://ssrn.com/abstract=1562461
Roon, M. (2016), Schlichtung und Blockchain, Anwaltsrevue 2016, 359-363, Stämpfli Verlag AG
Scherrer, S. (2014), Münchener Anwaltshandbuch Erbrecht, 4th ed., C.H. Beck Verlag
Schlosser, R. (1998), Der Know-how-Vertrag, 3 sic! 269
Schroeder, J.L. (2015), Bitcoin and the Uniform Commercial Code, Cardozo Legal Studies Research Paper No. 458, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2649441
Szulewski, P. (2015), A contractual perspective on succession of digital assets, Jusletter IT of 25 September 2015, available at: http://jusletter-it.weblaw.ch/issues/2015/24-September-2015/a-contractual-perspe_9fbc7525d8.html__ONCE#sectionb64258e4-f483-4170-80a4-d6080b1ce8c1
Troller, K. (2005), Grundzüge des schweizerischen Immaterialgüterrechts, 2nd ed., Helbing & Lichtenhahn
von Weizsäcker, C.F. (1971), Die Einheit der Natur: Studien, Carl Hanser
Weber, R.H. (2003), Schweizerisches Bundesverwaltungsrecht, Band V: Informations- und Kommunikationsrecht, 2nd ed., Helbing & Lichtenhahn
Weber, R.H. / Chrobak, L. (2015), Der digitale Nachlass: Fragen der rechtlichen Zuordnung von Daten zu Lebzeiten und von Todes wegen, Jusletter IT of 24 September 2015, available at: http://jusletter-it.weblaw.ch/issues/2015/24-September-2015/der-digitale-nachlas_26cc785a00.html__ONCE
Weber, R.H. / Chrobak, L. (2016a), Online-Netzwerke als neue rechtliche Gemengelage, Jusletter IT of 25 February 2016, available at: http://richterzeitung.weblaw.ch/jusletter-it/issues/2016/IRIS/online-netzwerke-als_806b98eafd.html__ONCE
Weber R.H. / Chrobak, L. (2016b), Rechtsinterdisziplinarität in der digitalen Datenwelt, Jusletter of 4 April 2016, available at: http://jusletter.weblaw.ch/juslissues/2016/841/rechtsinterdiszip-lin_a921783932.html
Wiebe, A. (2016), Protection of industrial data – a new property right for the digital economy?, GRUR Int. 2016, 877
Wiegand, W. (2015), in: H. Honsell / N.P. Vogt / T. Geiser (Eds.), Basler Kommentar, Zivilgesetzbuch II, Article 457-977 ZGB, Article 1-61 SchlT ZGB, 5th ed., Helbing & Lichtenhahn
Yermeck, D. (2015), Corporate Governance and Blockchain, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2700475
Zech, H. (2012), Information als Schutzgegenstand, Mohr Siebeck

Personal Data After the Death of the Data Subject—Exploring Possible Features of a Holistic Approach

Mark-Oliver Mackenrodt

Contents

1 Introduction: Exemplary Scenarios for the Legal Treatment of Personal Data After the Death of the Data Subject ... 274
1.1 The Inductive Character of a Holistic Approach ... 274
1.2 Cases in Point for Post Mortem Access to Accounts and to Personal Data ... 275
2 Property Law and the Treatment of Personal Data Post Mortem ... 277
3 Intellectual Property and the Treatment of Personal Data Post Mortem ... 277
4 Data Protection and the Treatment of Personal Data Post Mortem ... 278
5 The Right of Personality and the Treatment of Personal Data Post Mortem ... 280
6 Data Portability and the Treatment of Personal Data Post Mortem ... 281
7 Contract Law and the Treatment of Personal Data Post Mortem ... 281
7.1 Exemplary Contract Clauses with Regard to Personal Data Post Mortem ... 282
7.2 Possible Imbalance of Interests and of Bargaining Power in a Contractual Agreement Regarding Data ... 283
7.3 Standards for the Legal Assessment of General Contract Clauses Regarding Data ... 283
7.4 Contractually Imposed Requirements Regarding the Legitimation of Heirs ... 285
7.5 Conclusions on Contract Law and Personal Data After Death ... 286
8 Inheritance Law and the Treatment of Personal Data Post Mortem ... 286
8.1 The Principle of Universal Succession and Formal Requirements ... 287
8.2 Inheritability and the Intangible Character of Personal Data ... 287
8.3 Inheritability and the Private Nature of Personal Data ... 288
8.4 Inheritability of a Personalized Contract? ... 290
8.5 Conclusions on Inheritance Law and Personal Data After the Death ... 291
9 Secrecy of Telecommunications and the Treatment of Personal Data Post Mortem ... 291
9.1 The Original Rationale of Telecommunications Secrecy and Its Three-Step Extension with Regard to OTT Services ... 292
9.2 Possible Exceptions to Telecommunications Secrecy with Regard to the Heirs ... 293

Mark-Oliver Mackenrodt, Dr., Dr., LL.M. (NYU), Attorney at Law (New York), is a Senior Researcher at the Max Planck Institute for Innovation and Competition.

M.-O. Mackenrodt (✉)
Max Planck Institute for Innovation and Competition, Munich, Germany
e-mail: mark-oliver.mackenrodt@ip.mpg.de

M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law*, MPI Studies on Intellectual Property and Competition Law 28, https://doi.org/10.1007/978-3-662-57646-5_11

10 Conclusions 294
10.1 The Exemplary Case and a Possible Holistic Approach 294
10.2 Possible Features of a Holistic Approach 298
References 300

Abstract This paper intends to explore possible features of a holistic approach to the legal treatment of personal data. The paper proceeds in an inductive way. As an exemplary scenario the legal treatment of personal data after the death of the data subject is examined. More specifically, recent cases with regard to heirs demanding access to a social media account and to the personal data therein after the death of the testator are analysed and used as a reference point for discussion. It is examined how property law, intellectual property law, privacy law, the right to personality, the portability provisions, contract law, inheritance law and telecommunications law deal with personal data after the death of the testator. Against this background, shortcomings, common features and possible synergies are identified which might be taken into account for developing a holistic legal approach to personal data.

1 Introduction: Exemplary Scenarios for the Legal Treatment of Personal Data After the Death of the Data Subject

This article seeks to explore possible features of a holistic legal approach to personal data. As an exemplary scenario the legal treatment of personal data after the death of the data subject is analysed with regard to different fields of law. More narrowly, the case of heirs seeking access to a social media account of the testator and to the personal data therein is used as a reference scenario.

1.1 The Inductive Character of a Holistic Approach

There is no special set of provisions, for example in inheritance law, which directly addresses these questions.[1] Rather, the legal treatment of personal data after death is essentially determined by the general legal provisions of different fields of law. Most of these provisions would similarly be applied to a traditional fact pattern which does not involve personal data. Accordingly, the overall legal approach results from the interaction of different fields of law, like for example contract law, inheritance law, data protection law, the right to personality and the provisions on telecommunications secrecy. Absent a specialized provision the interplay of these

[1] There are, for instance, no special provisions in Belgium: Maeschaelck (2018), 37 or Germany: Mackenrodt (2018), 41.

different fields of law constitutes an indirect regulation with regard to personal data after the death of the testator.

Given the dynamic and diverse character of possible scenarios and business models which involve personal data, drafting a single provision which comprehensively deals with personal data after the death of the testator seems highly complex and, at this time, premature. Probably this would not even be advisable. Rather, at this quite early point of the discussion, an inductive approach appears to be warranted which takes particular fact patterns as a starting point for developing general principles.

1.2 Cases in Point for Post Mortem Access to Accounts and to Personal Data

A recent case in point deals with heirs who are seeking access to a social media account and to the data stored therein. This topic has increasingly been the subject of academic articles,[2] books[3] and law commentaries.[4] Similar discussions can be observed in many jurisdictions.[5] Meanwhile, one of the first court cases in Germany dealing with access of the heirs to a social media account and to the personal data therein has been handed down. In this case the plaintiffs are the parents and heirs of a girl who died at the age of 15 years after a tram accident. During her lifetime, the underage daughter had handed over the access data to her facebook social media account to her mother. However, a few days after the girl's death the internet company had been informed by an anonymous third person about the girl's passing away and blocked the account by putting it into a so-called state of remembrance.[6] In the case at hand this meant that only people who were registered as "friends" of the deceased during her lifetime could continue to access the account and continue to write posts. The parents did not belong to this group of people. The parents sued facebook in order to obtain access to the account of their deceased daughter and to

[2] See for example Wellenhofer (2016), 653; Deusch (2016), 189; Gloser (2016a), 12; Salomon (2016), 324; Gloser (2015), 4; Herzog (2016), 173; Gloser (2016b), 548; Lange / Holtwiesche (2016a), 487; Podszun (2016), 37; Lange / Holtwiesche (2016b), 125; Mackenrodt (2018), 41; Bock (2017), 370; Alexander (2016), 301; Raude (2017), 17; Steiner / Holzer (2015), 262; Nemeth / Carvalho (2017), 253; Kuntz (2016), 398.

[3] See for example Kutscher (2015); Katharina Seidler (2015); Bräutigam (2014), Anhang Digitaler Nachlass; Gebauer (2015).

[4] See for example Müller-Christmann (2017), § 1922 para. 99 et seq; Leipold (2017), § 1922 para. 24 et seq; Preuß (2017), § 1922 para. 375 et seq; Kunz (2017), § 1922 para. 594 et seq.

[5] See for example Nemeth/Carvalho (2017), 253; with a focus on the UK law: Harbinja (2017), 253; with a focus on Belgium: Maeschaelck (2018), 37; with a focus on the Netherlands see Berlee (2017), 256; with a focus on Austria see: Gebauer (2015). See also the consultation paper of the UK Law commission on making wills: Law Commission UK (2017).

[6] The features of the memorial status are subject to change. A recent description of its properties can be found with Harbinja (2017), 254, 255.

the messages stored within the account. By gaining access to their deceased daughter's facebook account the parents were hoping to obtain information about a possible suicide of their daughter and to avert possible damage claims by the tram driver.

The Landgericht Berlin[7] (LG Berlin) as court of first instance discussed provisions of several fields of law and concluded that the parents were entitled to be granted access to the facebook account. On appeal the Kammergericht Berlin[8] (KG Berlin) as court of second instance rejected the claim. The KG Berlin argued that allowing access of the original account owner's heirs to the facebook account would be in contradiction to the provisions which protect the secrecy of telecommunications. Using this argument from telecommunications law the KG Berlin widely left open the substantive treatment of social media accounts and of personal data after the death of the testator by other fields of law. Because of the fundamental importance of the legal issues raised in the case the KG Berlin admitted an appeal of its decision to the German Supreme Court (Bundesgerichtshof, BGH).[9]

This case, of course, only touches upon a subset of questions which may arise with regard to the legal treatment of personal data after the death of the data subject. In particular, the question whether the heirs can be granted access to certain parts of the account instead of access to the account as a whole has not been dealt with by the courts. Still, this case can in several respects serve as a point of reference for the discussion of a holistic approach in an exemplary way.

In a broader perspective, access of the heirs to accounts and to personal data plays a role in a wide range of quite different fact patterns. In a broad sense the questions raised concern all legal relationships of the deceased person with regard to digital assets.[10] This includes for example access to cloud storage or to cloud software, access to e-mails, rights with regard to websites, rights with regard to cryptocurrency, access to an online music library, access to platforms in general and contractual relationships and licensing agreements with regard to online works.[11] These positions are not merely of personal or sentimental character. Rather, they may represent considerable economic values. This is evident in the case of digital currencies, online tickets to concerts, credit balances with payment services such as paypal and credit balances with platforms such as ebay. For businesses as well, ongoing access to internet platforms can be of vital importance[12] and constitute the core of an enterprise. Companies are increasingly organizing their sales and distribution via platforms and moving core business units and essential business data into cloud systems.

---

[7] LG Berlin, judgment of 17 December 2015 - 20 O 175/15.

[8] KG Berlin, judgment of 31 May 2017 - 21 U 9/16, 24.

[9] BGH, judgment announced for 12 July 2018 - III ZR 183/17.

[10] Raude (2017), 19; Bräutigam (2014), Anhang Digitaler Nachlass, para 3; Deusch, (2014), 2; Maeschaelck (2018), 38.

[11] Further examples can be found in Alexander (2016), 302; Gebauer (2015), 69 et seq; Berlee (2017), 256.

[12] Raude (2017), 17.

2 Property Law and the Treatment of Personal Data Post Mortem

Property law, in general, enables heirs to be handed over all "things" in the sense of property law which were owned by the testator. If personal data are stored on hardware which was owned by the testator, the ownership of the hardware is—according to the law of inheritance—transferred to the heirs after the death of the testator. This transfer of ownership of the physical good to the heirs goes along with a transfer of the digital goods which are stored on the hardware devices, like for example e-mails, digital pictures, files and personal data.[13]

If personal data are not stored on hardware which was owned by the testator the question arises whether property law in combination with inheritance law would allow the heirs to obtain a legal position with regard to the personal data of the testator. Data as such and also an account as such do not have a corporeal character and, therefore, do not qualify as a "thing" in the sense of property law. Therefore, according to the general principles, property law does not apply to personal data, neither before nor after the death of the testator.

3 Intellectual Property and the Treatment of Personal Data Post Mortem

Even though property law does not apply to personal data, data as such might be the object of an intellectual property right, in particular of a copyright. For example, there might be a copyright of the deceased person with regard to digital photos, digital paintings or a written work like a poem or a post in a blog which is saved in a file or in a social media account.

A copyright constitutes an absolute right with regard to the copyrighted work and is independent of a property right which exists with regard to the hardware on which the data are saved. Independent of the ownership position with regard to the physical data carrier, a copyright constitutes a separate and additional legal position with regard to the data and to the digital content.[14] If the copyright-protected data are not saved on hardware owned by the testator but for example in a cloud, the testator still has an absolute right in the copyrighted data. German copyright law explicitly stipulates in § 28 UrhG (German Copyright Act) that copyrights are inheritable.

However, with regard to personal data the application of existing copyright is of limited reach for several reasons:

A copyright grants its owner and subsequently her heirs certain exploitation rights, like for example the right to copy or to license the work, and gives the author the right to interdict such exploitation by others. Accordingly, the heir would be able to interdict actions of an internet company only if these actions are to be qualified

[13] Alexander (2016), 303; Raude (2017), 19.

[14] Stresemann (2017), § 90 para. 25.

as acts of exploitation in the sense of copyright law. Therefore, copyright alone might prove to be a rather weak instrument for achieving access to data or to an account or for achieving an erasure of data or of an account. § 25 II UrhG explicitly states that the person who is in possession of a copyrighted work is under no obligation to hand the work or a copy of the work over to the copyright holder. Only under certain conditions laid down in § 25 I UrhG can the copyright holder obtain access to the work, for example in order to make a copy.

Further, a copyright with regard to personal data would require that the legal requirements for obtaining a copyright are fulfilled. In particular, a certain level of originality has to be demonstrated. Personal data will in many cases not meet these criteria and, therefore, only very seldom actually be the subject of a copyright.

However, copyright is just one kind of intellectual property right. For data as such, the creation of a specific intellectual property right by the legislature has been discussed in academic articles[15] and in a recent communication[16] by the European Commission. Currently however, data as such are not the subject of such an absolute right[17] and, also, in a more recent communication by the European Commission there seems to be a shift in focus towards the discussion of access rules and away from the creation of a special property right with regard to data as such.[18] One rationale of intellectual property law consists in assigning intangible goods to a particular person. The discussion about extending intellectual property rights protection to data as such shows that in some aspects this rationale also applies to data. However, such a right might also have adverse effects and not cure a perceived market failure.

In sum, an intellectual property in personal data would be transferred to the heirs. However, copyright will rarely apply to personal data and currently an absolute intellectual property right for personal data as such does not exist.

4 Data Protection and the Treatment of Personal Data Post Mortem

Personal data are the main subject of data protection law. However, the European General Data Protection Regulation (GDPR)[19] in its recitals 27 and 158 explicitly declares that the Regulation does not apply to the personal data of deceased persons.

[15] An overview of this debate on the creation of an ownership in data and a critical assessment can for example be found in Drexl (2017), 340 et seq.

[16] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 'A Digital Single Market Strategy for Europe' COM (2015) 192 final, 15, 20. The European Commission is announcing to (among other topics) address the emerging issue of data ownership. See also Zech (2015), 1151.

[17] Maeschaelck (2018), 37, 38 with regard to the Belgian law.

[18] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 'Building a European data economy' COM (2017) 9 final, 8.

[19] Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the

Further, the Regulation expressly leaves it to the Member States to regulate the legal treatment of personal data after the death of the data subject.[20] In Germany,[21] the UK[22] and in Belgium[23] for example, the data protection rules explicitly only apply to living individuals. This can be explained with the classical objective of data protection law to safeguard the autonomy of the individual to plan and pursue his life. This traditional forward-looking rationale of privacy law is not or not fully applicable after the death of a person. In this conception the right to privacy is a subcategory of the personality right which expires with the death of the person and which is not inheritable.[24] Still, even without an application of the privacy rules the deceased person would after her death be protected for example by the post mortem personality right.[25] But for this right to apply there would have to be a disfigurement of the memory of the deceased person.

The right to be forgotten as laid down in Art. 17 GDPR already constitutes an extension of the traditional privacy law. Further, some countries have been reported to have extended the application of their national privacy rules to deceased persons[26] or that such changes have been proposed.[27] In these instances the traditional rationale of privacy law has also been expanded. It would, however, need to be discussed by whom such a right would be administered after the death of the data subject. The next of kin might be better suited for this role than the internet company. In any case, the next of kin will usually be identical with the heirs, and in order to administer the right they might need knowledge of the personal data.

In sum, data protection in favour of a deceased person would under German law not constitute an obstacle to granting the heirs access to the account of the testator and the personal data.[28]

An internet account may, in addition, contain personal data of third persons who are still alive. However, this would in many cases not present an impediment to allowing heirs access to the account. According to Article 2, 2. (c) GDPR the data protection rules do not apply to the processing of personal data in a private context. Further, under inheritance law[29] the heirs have a right of surrender against every person who is in possession of objects which form part of the estate. Accordingly, a paper-based address book of the testator which contains personal data of third

---

free movement of such data, and repealing Directive 95/46/EC, OJ L 119/1, 4 May 2016 (GDPR).

[20] GDPR, recital 27.

[21] Bock (2017), 398.

[22] Harbinja (2017), 255.

[23] Berlee (2017), 259.

[24] Berlee (2017), 259.

[25] For a discussion see 5.

[26] With regard to France and Hungary reported by Harbinja (2017), 255; with regard to France see also Chrobak (2017), recital 10.

[27] A proposal with regard to Swiss law is reported by Chrobak (2017), recital 10.

[28] Bock (2017), 402.

[29] A discussion of inheritance law and personal data can be found below 8.

persons and which is in the possession of a person other than the testator would have to be handed over to the legitimate heirs. With regard to an online address book the legal assessment should not be different.

Finally, the result would not be different even if handing the personal data over to the heirs were interpreted as a processing of data on the part of the internet company. According to Article 6, 2. (c) GDPR a processing of data is lawful if it is necessary for complying with a legal obligation. As inheritance law requires that all assets be handed over to the heirs, inheritance law might serve as a sufficient legal basis in the sense of the GDPR.[30]

In any case, if the heirs use personal information about third living persons in a discrediting way this person is protected by his right to personality.

5 The Right of Personality and the Treatment of Personal Data Post Mortem

Personal data can be protected by the right to personality. According to the German legal doctrine the right to personality is of a dual character. The commercial elements of the personality right, like for example the right to commercially exploit the picture or the voice of a person, is inheritable and does not have constitutional character.[31] By contrast, its personal element, which for example protects the honour of a person, is of constitutional rank. Due to its highly personal character it expires with the death of the person and is not inheritable.[32] However, also a postmortal right of personality[33] is recognized. For a time of 10 years it protects the deceased person against gross distortions of the memory regarding the deceased person. This right is administered by a fiduciary designated by the deceased person or, absent such a designation by the close family members, the next of kin. Such fiduciaries can for example seek injunctive relief under tort law.[34]

The handling of personal data of a deceased person can affect the commercial right to personality. Only the commercial aspect of the personality right is passed on to the heirs. By contrast, the postmortal right to personality can only be invoked if the use of the data constitutes a disfigurement. Granting heirs access to the personal data of the deceased and to his social network account as such does not infringe the postmortal right of personality.[35] Also, the heirs are often identical with the next of kin who are in most cases the fiduciaries who exercise this postmortal right.

[30] For a discussion of inheritance law and the relationship to privacy issues see below 8.3.

[31] Preuß (2017), recital 352, 360; Bock (2017), 387.

[32] Preuß (2017), recital 353, 367.

[33] Bock (2017), 389; Preuß (2017), recital 353, 368.

[34] Preuß (2017), recital 363.

[35] Bock (2017), 395.

In sum, the mere perception of personal information by the heirs does not constitute a disfigurement of the personality of the testator or of a third person and, therefore, does not infringe their rights to personality.

6 Data Portability and the Treatment of Personal Data Post Mortem

The right to data portability seeks to enable users to take their data with them when they terminate a contract with an internet platform, and to encourage users to switch platforms. A right to data portability can, for example, be found in Article 20 of the European General Data Protection Regulation and in the proposal for a Directive on certain aspects concerning contracts for the supply of digital content.[36] The provisions serve to strengthen the position of the user, safeguarding his autonomy over his data, and to promote competition between platforms by lowering switching costs. The GDPR does not directly apply to personal data of deceased persons. However, the provisions, in particular those in the proposed digital content directive, and their rationale might be of relevance when the heirs, as living persons, want to move the account to a different platform, or in the evaluation of agreements which lead to the de facto result that accounts become orphaned and continue to be commercially exploited by an internet company.

More generally, it has to be noted that the rationale of the data portability provisions is specially tailored to the particular market conditions and to possible dangers in the data economy. Therefore, within a holistic approach the objectives of data portability should be attributed high priority.

7 Contract Law and the Treatment of Personal Data Post Mortem

The legal treatment of personal data after the death of the data subject has also to be determined with regard to contract law. After all, only objects which actually form part of the estate at the time of the testator's death are passed on to the heirs. Inheritance law does not create new legal positions[37] but provides for a succession of the heirs into certain legal positions of the testator. It follows from the legal principle of freedom of contract that during his lifetime the testator is free to dispose of

[36] Proposal for a Directive of the European Parliament and of the Council of 9 December 2015 on certain aspects concerning contracts for the supply of digital content COM(2015) 634 final.

[37] Chrobak (2017), recital 3.

his assets.[38] For example with regard to social media platforms, there are often contractual agreements between the testator and the social media platform which relate to the account and to the personal data in the account after the death the holder of the account. Such an agreement could de facto exclude an asset from being passed on to the heirs by way of inheritance law.

7.1 Exemplary Contract Clauses with Regard to Personal Data Post Mortem

In their general terms and conditions, platform operators address the post mortem legal treatment of the account and of data in very different ways.[39] One social network, for example, stipulates that data and content become the property of the platform as soon as they are posted, or that in the event of death they remain permanently with the network without the possibility of deletion for the testator and her heirs. Already at first glance it seems problematic that by way of contract the platform seemingly seeks to establish property in its favour with regard to data of the account owner even though such a property right may not exist and even though the current discussion rather intends to strengthen the data subject and not the platform owner by creating an intellectual property right in data. As another example, the terms and conditions of a large cloud storage provider state that stored content is non-transferable and expires upon death. Also, an automatic deletion after death can be provided for. The general terms and conditions of another large e-mail service try to establish a non-transferability of the account and a termination of all rights. Some general terms and conditions reserve for the e-mail provider or the messenger service a right of discretion for the case that the cancellation of an account or the deletion of a message is requested. In this case the will of the internet company would supersede the will of the testator and her heirs.

Contractual agreements can also seek to create high formal hurdles for the heirs, so that heirs are discouraged from taking action or asserting their rights. For example, a large e-mail provider requires the submission of a certificate of inheritance. Another e-mail provider demands that a death certificate be presented and, in addition, a court order which has to be issued by an Irish court and to be expressly addressed to the e-mail provider. With such strict formal requirements it is unlikely that heirs will successfully seek access to the data of the testator or to an account which would also allow them to delete the data and the content and to finally close the account.

[38] Lange / Holtwiesche (2016b), 128.

[39] Examples can be found in Lange / Holtwiesche (2016a), 488; Raude (2017), 21. Willems (2016), 496; Harbinja (2017), 254.

7.2 *Possible Imbalance of Interests and of Bargaining Power in a Contractual Agreement Regarding Data*

Contractual standard agreements of internet platforms are quite often characterized by an imbalance of interests. It should be noted that when drafting their general terms and conditions the internet companies—like every party to a contract—are guided by their self-interest. If, for example, personal data or an account of a deceased person are not or cannot be deleted, a social network can still continue to generate revenues with the data even if the account is in a memorial status. Even an orphaned account can still be profitable and generate internet traffic. This is, for example, shown by the fact that there are numerous commercial websites which offer digital services to commemorate deceased persons.[40] There, for example, posts written by friends or even by the deceased themselves during their lifetime can be published.

The general terms and conditions of a social network can have the effect that the personal data and the account of the deceased person remain as a default rule de facto and permanently assigned to the social network and that it can make use of the account and the data in its commercial self-interest. Also, the deceased and the heirs may not only be excluded from obtaining access to the personal data but de facto also from deleting the personal data.

At the same time, internet platforms often possess market power and a superior bargaining position when they—as a rule—unilaterally impose their general terms and conditions upon the users. The data holders on their part do not have an opportunity to enter into negotiations at eye level, and this leads to a market failure. In order to compensate for this market failure general terms and conditions are subject to a review by contract law. Under German law, general terms and conditions are subject to a legal review which is based on §§ 305 ff. BGB (German Civil Code). These provisions constitute an implementation of the European Unfair Contract Terms Directive 93/13.[41] The legislative purpose of this review mechanism is particularly pertinent with regard to internet platforms.

7.3 *Standards for the Legal Assessment of General Contract Clauses Regarding Data*

According to § 305c I BGB standardized contractual provisions do not become part of the contract if in the particular circumstances they are so unusual that the other party to the contract could not need to expect to encounter them. Further, standardized provisions are invalid according to § 307 I BGB if contrary to good faith they unreasonably disadvantage the other party. This is to be assumed if the clause is

[40] An overview of this industry is provided by Martini (2015), 35.

[41] Directive (EEC) 93/13 of the Council of 5 April 1993 on unfair terms in consumer contracts OJ L95/29, 21 April 1993.

incompatible with statutory provisions from which it deviates or if essential rights are limited to an extent that the attainment of the purpose of the contract is jeopardized.

When assessing agreements which relate to the personal data the question arises which model of contract typology is to be used as a benchmark. In most cases such contracts cannot easily be classified as being attributable to a single type of contract. Rather, they contain multiple elements which are characteristic for several of the contract types which are regulated by law. Cloud storage services, for example, exhibit elements of rental agreements and of service agreements. In the case of e-mail services, not only the storage of messages but also the service of message management is the subject of the contract. Developing a legal standard for assessing contracts of mixed typology is very complex and requires a normative and objective balancing of the rights and obligations which are established by the contract.[42] If a contractual provision deals directly with the processing of personal data, like for example with questions of consent, transparency and justifications, the GDPR can serve as a benchmark for a review of these contractual agreements.[43]

A further controversial question gains significance for agreements which relate to the treatment of personal data after the death of a person. The legal assessment of a standardized contract involves a balancing of the interests of the persons who are parties to the contract. As the heirs are originally not a party to the agreement, the question arises whether their interests as a third party can or have to be taken into account in the review of the contractual clauses. As to the prevailing opinion the interests of third parties and persons not directly involved in the contract are not to be directly considered within the balancing process.[44] However, indirectly interests of third parties play a role if they coincide with the interests of a party to the contract.[45] This can be the case for heirs and testators, for example, with regard to preserving their property or preserving control over the data.

There are several reasons why a standardized agreement could be deemed as invalid if it leads to an automatic deletion of the data[46] or of an account by the internet company or if it would lead to the existence of orphaned personal data or to orphaned accounts or a contractual stipulation would provide for access to the account only at the discretion of the internet company.[47]

In a rental agreement, for example, returning the stored good at termination of the contract would be a contractual obligation which is essential. Outside the digital context, the heirs also have to be granted access to a banking account and to a

[42] For further details see for example Fuchs (2016), § 307 para. 239.

[43] For a thorough discussion see for example Wendehorst / Graf von Westphalen (2016), Graf von Westphalen (2017).

[44] Fuchs (2016), § 307 para. 133.

[45] Wurmnest (2017), § 307 para. 50.

[46] An agreement which provides for an automatic deletion of an account considered as invalid by many authors, see Gloser (2016a), 13; Alexander (2016), 306; Raude (2017), 20; Lange / Holtwiesche (2016b), 128; Gloser (2016b), 548; Herzog (2013), 3751.

[47] A legal assessment of different standardized agreements can be found with Seidler (2015), 143 et seq; Kutscher (2015), 116 et seq.

storage room. Quite similarly, the purpose of a platform or cloud contract consists in storing data and having access.

In addition, a permanent de facto assignment of the orphaned data to the internet companies would be in conflict with emerging general legal principles of the data economy. It can be concluded from the provisions on data portability[48] that the lawmakers wanted the user to retain control of his data and not the internet company. Also, given that there are commercial memorial platforms the ratio of the data portability provisions applies in the sense that also competition between such platforms should be furthered by alleviating the possibility of switching platforms. A similar argument can be drawn from the discussion on the introduction of an ownership right in data.[49] The intended beneficiary of such a right would not be the internet company. Finally, a contractual provision would be void according to which the social media account can be put into the state of memorial on the basis of a simple notice by a third party.[50] In this case an arbitrary third person would be allowed to decide whether the account holder or his heirs can continue having access to the account.

7.4 Contractually Imposed Requirements Regarding the Legitimation of Heirs

General terms and conditions of internet platforms often seek to establish requirements for the heirs to proof their legal status as heirs when they seek access to personal data or to an account of the testator.[51] Concerning such legitimation requirements for heirs the case law of the German Federal Supreme Court (BGH) regarding banking accounts can be invoked.[52]

In one case[53] the general contractual agreements between the bank and the testator required that after the death of the testator the heirs would only be allowed access to the account if they present an inheritance certificate. Even if the heir could present a public will of the testator and even if there was no doubt as to his position as an heir the general terms and conditions of the bank did solely allow a court-issued inheritance certificate as a document of proof. The BGH declared such an agreement in the general terms and conditions as invalid.

Quite similarly, the general terms of conditions of online platforms which require heirs who seek access to present an Irish court order issued to the platform is likely to be invalid.[54] Such a requirement would de facto render the heir's access to the

[48] For data portability see 6.

[49] For the discussion on a possible data ownership see 3.

[50] Leipold (2017), para 29.

[51] For further examples see 1.

[52] See also Deutscher Anwaltsverein (2013), 62 et seq.

[53] BGH, IX ZR 401/12, 8 October 2013.

[54] Lange / Holtwiesche (2016a), 489; Raude (2017), 23.

inheritance more difficult and diminish the ability of the testator and of the heir to determine the fate of the inheritance. This right, however, forms part of the constitutional guarantee of property.

In the facebook case decided by the LG Berlin the general terms and conditions stipulated that any third person could report the account owner's death to facebook and that the account would then be put into the memorial state. Thereby, the account would irrevocably be closed for the heirs even if they could establish their status as heirs of the account. The LG Berlin declared that such a provision does not sufficiently assure that the testator or the heir can decide on the fate of the account.[55]

7.5 Conclusions on Contract Law and Personal Data After Death

Contractual agreements can influence which assets and data are considered to be still part of the estate at the time of the death of the testator. However, general terms and conditions are subject to a legal review. With regard to legitimation requirements for heirs who want to claim their inheritance existing jurisprudence relating to banking accounts can be invoked. However, many questions remain unsettled, in particular because in many instances it is difficult to determine a normative benchmark for balancing the diverging interests.

The legal control of general terms and conditions is justified by the fact that standardized contract clauses are in general not negotiated at eye level, are unilaterally imposed by one party and more than likely not sufficiently taken note of in detail. This justification is particularly pertinent when it comes to contractual agreements which are concluded on the internet and which deal with the handling of personal data. Accordingly, the nature of personal data does not speak against an application of the review of contractual obligations. To the contrary, such a review is even more warranted with regard to personal data. This reasoning is supported by the fact that the General Data Protection Regulation also imposes special rules with regard to transparency and with regard to the validity of the data subject's consent. As a consequence, in a holistic approach this common objective of contract law and data protection law should be accorded substantial weight.

8 Inheritance Law and the Treatment of Personal Data Post Mortem

The legal treatment of data after death is in particular to be analysed from the viewpoint of inheritance law.

[55] LG Berlin, judgment of 17 December 2015 - 20 O 175/15B. II. 2. e.

8.1 The Principle of Universal Succession and Formal Requirements

Inheritance law, for example in Germany,[56] Belgium[57] and the Netherlands,[58] generally adheres to the fundamental principle of universal succession. Universal succession means that the deceased person's estate is automatically passed on as a whole to the heirs. As a rule a separate transfer of individual assets to the heirs is not required. Rather, the heirs by operation of law step into the legal positions of the testator. The heirs have a claim to surrender with regard to all assets which constitute a part of the estate.[59]

An essential prerequisite for the inheritability is that a particular asset forms part of the estate at the time of death. Therefore in the case of a legally effective contractual disposition of the testator during his lifetime with regard to a particular asset, this asset is not passed on to the heirs by way of universal succession. However, as shown above contractual agreements with regard to data are subject to certain requirements. Also, if such a disposition is to be qualified as a disposition upon death[60] the formal requirements of inheritance law may apply. If the formal requirements are applicable but not complied with the disposition is void. Currently it is not recognized that digital technology can fulfil the formal requirements of inheritance law.[61] In inheritance law the formal requirements serve a warning function. They seek to make the testator aware of the reach and the importance of his actions and to create legal security. This objective is in particular and even more applicable with regard to personal data. Therefore, within a holistic approach this rationale should be given room.

Regarding a holistic approach to the application of inheritance law to personal data three main issues need to be discussed—the intangible character of personal data, their personal character and the possibly customized character of the underlying contractual relationship.

8.2 Inheritability and the Intangible Character of Personal Data

The first question is whether the lack of physicality of data or of a social media account constitutes an obstacle to inheritability.

---

[56] See § 1922 BGB.

[57] See Maeschaelck (2018), 40.

[58] See Berlee (2017), 256.

[59] Lange / Holtwiesche (2016b), 162.

[60] The distinction between a disposition during lifetime and a disposition upon death is in general discussed by for example Müller-Christmann (2017), § 1937 para. 3.

[61] Harbinja (2017), 254; Maeschaelck (2018), 41.

Corporeal "things" in the sense of property law like for example a data carrier are passed on to the heirs. As discussed above[62] according to § 28 UrhG (German Copyright law) copyrights are also inheritable.[63] Accordingly, the law does expressly clarify that the intangible character of the copyright does not exclude its inheritability.

However, the existence of an ownership position with regard to data is not even a prerequisite for digital assets to be inheritable. The inheritance-law principle of universal succession does not only apply to ownership positions but also to contractual rights of the deceased person.[64] Access to data which are saved in an account, a platform or a cloud storage is based on a contractual relationship between the provider of the service and the testator.[65] This includes a contractual claim of the deceased person to obtain access. Such a legal position forms part of the "estate" within the meaning of § 1922 I BGB and is therefore passed on to the heirs according to the principle of universal succession.[66] It should be noted that the discussion of creating a data ownership is not limited to the time before the death of a person.[67] At the same time, it becomes clear that the inheritability of access to a social media account or to personal data can be implemented without creating an ownership right in data. However, in some instances property law might provide a stronger legal position than a contractual claim, like for example in case of a bankruptcy.[68]

In sum, the intangible character of data or of a social media account do not constitute an obstacle to inheritability. Further, a contractual relationship which forms a basis for access to data is inheritable.

8.3 Inheritability and the Private Nature of Personal Data

It further needs to be analysed whether the private nature of personal data or of a social media account constitutes an obstacle for the inheritance law principle of universal succession to apply. Some legal positions are not inheritable due to their highly personal character, such as a human rights position, a right to unemployment benefits or the personal element of the right of personality.[69] By contrast, the commercial element of the right of personality is inheritable. In addition there is a post-mortal right of personality to protect the deceased person against disfigurements of his memory after his death.

---

[62] For a discussion on personal data and intellectual property law see 3.

[63] For the inheritability of the author's right in Belgium see Maeschaelck (2018), 39.

[64] Leipold (2017), § 1922 para. 20.

[65] Fort he UK Harbinja (2017), 254.

[66] For a similar solution under Belgian law see Maeschaelck (2018), 40.

[67] Chrobak (2017), recital 1.

[68] Maeschaelck (2018), 40.

[69] For dual character of the right to personality consisting of a personal element and a commercial element see 5.

With regard to social media accounts it is discussed whether access of the heirs to the account and to the data therein should be denied because it may contain content which is personal in nature.

According to some authors, such accounts, data and e-mails should not be inheritable.[70] Otherwise—these authors claim—there would be a conflict with the testator's postmortal right of personality. Rather, such content should be forwarded to the next of kin who are administering the deceased person's postmortal right of personality.[71] This view would entail severe practical problems[72] as for example e-mails would need to be separated into different categories depending on their content. E-Mails with business character would have to be forwarded to the heirs while e-mails of more personal character would need to be passed on to the next of kin. Furthermore, it would not necessarily serve to protect the postmortal personality right of the testator if an internet company—or even a subcontractor—were to be entrusted with such a separation of personal and non-personal e-mails.

According to the predominant view the inheritability of a digital asset is not to be determined depending on the content of the data or its possible private character.[73] In several instances, German inheritance law does not provide for a special treatment with regard to objects which are of personal character. Rather, the law explicitly treats personal objects as part of the estate which are to be passed on to the heirs. For example, § 2047 II BGB stipulates with regard to the distribution of the inheritance among the heirs that documents referring to the personal circumstances of the testator remain common to the heirs. Thereby, the law presupposes that the principle of universal succession applies to such documents notwithstanding their highly personal character. Further, regarding the sale of an inheritance as a whole, § 2373 II BGB provides that in case of doubt family papers and family pictures are not considered to be sold and remain with the heirs. The law thus accepts in both regulations that even highly personal contents are passed on to the heirs.[74] Therefore, paper-based letters and diaries, for example, are to be handed over and can be read by the heirs without restriction.[75] A different handling of digital letters and digital diaries is not justified. This view is not in contradiction with the postmortal right of personality. The postmortal personality right is administered by the close relatives of the deceased person. If the close relatives are not identical with the heirs the close relatives can still (and only) take legal action if for example the testator's life picture is disfigured by the publication of personal information by the heirs.

---

[70] Hoeren (2005), 2114.

[71] Hoeren (2005), 2114.

[72] Deutscher Anwaltsverein (2013), 52.

[73] See for example Solmecke/ Köbrich/ Schmitt (2015), 291; Salomon (2016), 326; Klas / Möhrke-Sobolewski (2015), 3474; Raude (2017), 19; Lange / Holtwiesche (2016b), 126.

[74] Steiner / Holzer (2015), 263; Herzog (2013), 3748; Gloser (2016a), 16; Raude (2017),19; Alexander (2016), 303.

[75] Leipold (2017), para. 24.

In the case discussed, the KG Berlin left the question open whether the inheritability of the facebook account is excluded due to its possibly personal character.[76] In this case the parents were not only the heirs but also the legal guardians of their deceased daughter. Therefore, they were also administering their deceased daughter's postmortal right of personality.

8.4 Inheritability of a Personalized Contract?

Access to personal data and access to a social media account is often based on a contractual agreement. The inheritability of a contractual obligation could be excluded if the contractual relationship is personalized and specifically tailored to the testator. § 399 first example BGB excludes an assignment of rights if through a change of the contractual party the content of the contractual performance would be significantly altered.

This rule does not, for example, exclude the inheritability of the contractual right to use a particular domain name.[77] Also the courts have ruled that this argument does not exclude the inheritability of a social media account.[78] The contractual performance of a social network consists in providing the technical infrastructure of a communication platform. This service is not specifically modified for the person of the testator. In addition, membership in a social platform does not even include an identity check. Furthermore, in the case decided by the LG Berlin and by the KG Berlin the heirs were not seeking continuation of the account but access to its content.[79] In a case regarding banking accounts, the German courts have distinguished between the heirs' access to the money and the continuation of the banking account contract by the heirs.[80] Only the latter can be denied by the bank because of the possibly personal character. Quite similarly, with regard to a social media account one needs to distinguish between access to the account and the personal data therein on the one hand and the continuation of the contract on the other hand. Only the continuation of the contact might possibly if at all be denied on the grounds that the service contract was customized to the person of the testator.

[76] KG Berlin, judgment of 31 May 2017 - 21 U 9/16, 24.

[77] For the legal situation in Belgium Maeschaelck (2018), 40.

[78] KG Berlin, judgment of 31 May 2017 - 21 U 9/16, 20; Lange / Holtwiesche (2016b), 129 who point to the fact that the social network business is aimed at a high number of people in a standardized way.

[79] This distinction is also made by Herzog (2013), 3749; Gloser (2016a), 14.

[80] The comparison with banking accounts is made by Bräutigam (2014), Anhang Digitaler Nachlass, para 5.

8.5 Conclusions on Inheritance Law and Personal Data After the Death

Summing up, the general principles of German inheritance law allow for several insights into possible features of a holistic approach. Several objectives of inheritance law and several decisions of the lawmaker are particularly pertinent with regard to personal data:

The inheritability of digital assets is not to be excluded because personal data are of intangible character. Further, the ratio of the formal requirements is all the more applicable to personal data and to digital assets, which both may be of considerable economic value. Inheritance law is concerned with the succession of the heirs into the economic position of the successor. Therefore, economic aspects of the right to personality are inheritable. With regard to the inheritability of personal letters and family pictures, inheritance law shows that the personal character of an asset does not constitute an obstacle to inheritability. If and only if such personal information is used to disfigure the memory of the testator, is the testator protected by the post-mortal right to personality. Third parties are also protected by the right to personality against a misuse of their data by the heirs.

The contractual relationship in the course of which data are stored is generally not customized to the person of the testator. Therefore, an inheritability is not excluded. Even if there is a mass tailored contractual relationship a distinction has to be made between the continuation of the contract and access of the heir to the personal data.

9 Secrecy of Telecommunications and the Treatment of Personal Data Post Mortem

Personal data are often not saved on the hardware of the testator but on hardware which is owned by the service provider or for example in a cloud storage. Accessing these data requires a transmission of the data. In many instances, like in the example of a social media account or an e-mail account, there is a transmission involved between a third person and the service provider and the testator. Even if inheritance law and the contractual agreements required that the heirs be granted access to the account and to the personal data of the testator, this might be prevented by the rules on the secrecy of telecommunication. In this event, the protection of the telecommunication secret would override the objectives of inheritance law and contract law.

It is, however, disputed whether and to what extent the provisions on the secrecy of telecommunications are applicable for example with regard to social media account in which personal data are saved. In the German facebook case the LG Berlin did not regard the secrecy of telecommunications as an obstacle to granting

the heirs access to the social media account and the personal data.[81] By contrast, the KG Berlin as court of second instance dismissed the case, arguing that the provisions on the secrecy of telecommunications did apply.[82] The KG Berlin admitted an appeal to the BGH (German Supreme Court), where the case is still pending.

9.1 The Original Rationale of Telecommunications Secrecy and Its Three-Step Extension with Regard to OTT Services

In Germany, the secrecy of telecommunications is constitutionally protected by Article 10 GG (Grundgesetz, German Constitution) and according to statutory law by § 88 TKG (German Telecommunications Act). However with regard to a social media account or to personal data saved with an internet platform, these rules are only applicable through a three-step extension of the interpretation of these provisions.

Firstly, the constitutional right in Article 10 GG originally served as a safeguard against measures by the government. However, this provision is interpreted as also having a direct horizontal effect between private parties. Therefore, Article 10 GG and correspondingly § 88 TKG are deemed to be applicable to the relationship between a private internet company and the heirs.

A second expansion of the provisions of telecommunications secrecy has occurred in the sense that it is not required that the company itself is transmitting signals. The rationale of protecting the secrecy of telecommunications is grounded in the fact that the technical process of the transmission of the signals is particularly vulnerable to a secret or open intervention. Accordingly, the provisions on telecommunications secrecy were originally designed—and have ever since remained unchanged—to protect against interferences with the technical transmission infrastructure by the state.

An internet platform like a social network or an e-mail service is to be categorized as a so called OTT communication service (over the top communication service).[83] OTT companies solely offer software services to their customers and not the transmission of signals through a telecommunications infrastructure which they own themselves. Rather, internet platforms and their customers make use of the transmission lines of a separate company like an internet provider or a traditional telecommunications enterprise. However, in an earlier case the German Bundesverfassungsgericht (Federal Constitutional Court)[84] ruled that the provisions on the protection of the telecommunications secrecy are also applicable to OTT

[81] LG Berlin, judgment of 17 December 2015 - 20 O 175/15 B. II. 2. e.

[82] KG Berlin, judgment of 31 May 2017 - 21 U 9/16, 45.

[83] On OTT services and the German telecommunications law see Deusch / Eggendorfer (2007), 96 et seq.

[84] BVerfG, judgment of 16 June 2009 - BvR 902/06.

service companies. In this case a state authority had—as part of criminal proceedings—confiscated e-mails which were saved on the server of an e-mail service company.

An extensive interpretation of the provisions on telecommunications secrecy has occurred in a third sense. According to the German Bundesverfassungsgericht (BVerfG) the application of these rules is not limited to protecting the dynamic process of an ongoing telecommunications process.[85] Rather, also messages which have already been received and read by the addressee are protected if they are saved on the server of the OTT company even if the transmission to the addressee has already been completed. By contrast, if an e-mail is saved in the computer storage of the user the rules of telecommunications secrecy would not apply.

9.2 Possible Exceptions to Telecommunications Secrecy with Regard to the Heirs

In the court case where the heirs were seeking access to a social media account these three ways to extensively interpret the telecommunications provisions came into play in a cumulative manner. As a consequence of this cumulated extensive interpretation the LG Berlin[86] and the KG Berlin[87] ruled that the provisions on telecommunications secrecy were applicable to an OTT service provider like a social network.

It is however not undisputed whether the Telecommunications Act is at all applicable to social media. The German Federal Network Agency (Bundesnetzagentur) assumes since 2012 that for example an e-mail provider is subject to its regulatory power which is based on the German Telecommunications Act and on underlying European law. However, in 2018 a German court, the OVG Münster, referred the question to the European Court of Justice whether the telecommunications regulation is applicable to an e-mail provider.[88]

Even if the German Telecommunications Act and its provisions on telecommunications secrecy is deemed to be applicable a statutory exception might apply with regard to heirs seeking access to a social media account and to the data stored therein.

The LG Berlin—contrary to the KG Berlin in the second instance—found that an exception is applicable when it comes to allowing heirs access to a social media account. According to § 88 III 1 TKG, telecommunications service providers are permitted to inform themselves or others about the content of a communication if this is required for the provision of the telecommunications service. The LG Berlin

[85] BVerfG, judgment of 16 June 2009 - BvR 902/06, para. 47.

[86] LG Berlin, judgment of 17 December 2015 - 20 O 175/15 B. II. 2. e.

[87] KG Berlin, judgment of 31 May 2017 - 21 U 9/16, 30 et seq.

[88] OVG Münster – 13 A 17/16 see Press Release 26 February 2018.

argued that this exception was applicable because according to the law of succession the company was—as part of its business relationship—under a legal obligation to pass the data in the account on to the heirs.[89]

The KG Berlin[90] rejected this reasoning by pointing to § 88 III 4 TKG. This provision contains an exception to telecommunications secrecy with regard to certain particularly serious criminal offences. If such information can be found, the telecommunications company is under a legal obligation to pass this information on to the prosecution office. The KG Berlin concluded that only this legal duty, which is expressly specified by the TKG, would qualify for an exception. By contrast, for the fulfilment of other legal duties—like the duty to hand over the testator's assets to the heirs—no exception of the TKG would apply. This interpretation is to be reviewed by the BGH.

10 Conclusions

The discussion of the legal treatment of personal data after the death of the testator reveals with regard to the exemplary case and also in an overall perspective possible features of a holistic approach to personal data.

10.1 The Exemplary Case and a Possible Holistic Approach

Regarding access of the heirs to internet accounts and to personal data after the death of the testator, many legal questions may, at this time, remain unsettled and shortcomings and divergences in different jurisdictions are exhibited.[91] However, some guidelines for applying the different fields of law can be identified.

Data protection law is—in accordance with its traditional rationale—not applicable with respect to deceased persons. Regarding personal data of another living person, the privacy rules would in many cases also not be affected. For example the handing over of an address book to the heirs would in most cases not be subject to privacy law. After all, the testator and other persons who are still alive are protected by their (postmortal) right to personality if their data are used by the heirs in a way that disfigures their reputation. Therefore, data protection law[92] and the post mortem right to personality[93] are generally not considered to be an obstacle for the heirs to get access to personal data or to a social media account. Property and intellectual

[89] LG Berlin, judgment of 17 December 2015 - 20 O 175/15 B. II. 2. e.

[90] KG Berlin, judgment of 31 May 2017 - 21 U 9/16, 30 et seq.

[91] Chrobak (2017), recital 1.

[92] See for example Bock (2017), 397 et seq; Klas / Möhrke-Sobolewski (2015), 3473; Deusch (2016), 194; Knoop (2016), 969.

[93] See for example Bock (2017), 402 et seq.

property law are not, or only in a few cases, applicable to personal data, neither before nor after the death of the testator. The creation of a special intellectual property right in data as such is no prerequisite for inheritance law to apply, as the contractual claim to get access to the data is inheritable. Contractual agreements with regard to personal data are admissible and can affect the post mortem treatment of personal data. However, standardized agreements like general terms and conditions are subject to a legal review. With regard to personal data, the rationale of conducting such a review is particularly pertinent. Inheritance law shows that, according to its intended purpose, the intangibility of personal data is no obstacle to the application of inheritance law. Also, the decision of the lawmaker to expressly provide for an inheritability of analogue letters which may also contain personal information shows that the lawmakers considered privacy law as not standing in the way of applying inheritance law. A special treatment of digital messages is not warranted. The contractual claim to get access to the data is generally not customized to the testator in a way that would make the claim to access not inheritable. As in the example of banking accounts, one has to distinguish between the heirs' claim to access and a claim to continue the contract. As a rule, only the latter would be non-transferable.

With regard to telecommunications secrecy, the reach and the exceptions of the German rules are disputed when it comes to access of heirs to a social media account of the testator and to the personal data which are stored therein. A clarification by the German BGH as the third instance, or more generally by the legislature, is needed. The current interpretation of the provisions on telecommunications secrecy by the KG Berlin is in conflict with the underlying purpose of other fields of law and with the approach that is taken to personal data by other fields of law. In addition, this interpretation is not supported by the rationale of telecommunications secrecy itself. It has a blocking effect against granting access of the heirs to the account and to the personal data, even though the principles of the law of succession and of contract law require such access to be allowed and even though other fields of law do not stand in the way of granting access. The objectives of these fields of law would be superimposed and dispelled by the rules on telecommunications secrecy without good reason. There are several strands of arguments speaking against the KG Berlin's solution.

10.1.1 Conflict with the Principle of Universal Succession

The interpretation of the provision on telecommunications secrecy appears to be in contradiction with the inheritance-law principle of universal succession. According to § 1922 BGB the heirs by operation of law replace the testator and take over all her legal positions and obligations.[94] When the heir pursues her legal claim to be given the assets of the testator it seems contradictory to regard the heir as an "other person" in the sense of the provisions on telecommunications secrecy.[95]

[94] Alexander (2016), 303.

[95] Steiner / Holzer (2015), 264; Leipold (2017), para. 27.

10.1.2 The *Ratio Legis* as Inherent Limitation of Telecommunications Secrecy

It should further be taken into account that the principle of telecommunications secrecy is subject to inherent limitations which are derived from its own objectives. The secrecy of telecommunications protects the confidentiality of the process of communication because the communication partners themselves can only to a limited extent control this process. By contrast, telecommunications secrecy does not protect the confidential handling of a message by the recipient. The sender of a message cannot invoke the rules on telecommunications secrecy in order to prevent the recipient of a message from passing on the message to third persons. Quite similarly, in the field of analogue messages, the sender of a letter cannot invoke the postal service secret to prevent the letter's recipient from passing on the letter to third persons.[96]

In the case decided by the KG Berlin the underage daughter had during her lifetime passed on the login data of her account to her mother, who was her legal guardian. This situation should not be dealt with differently than a situation in which the messages have been saved on a local data drive or printed out and passed on to the mother by the testator himself or by way of universal succession.

If a testator does not want that the contents of a letter to come to the knowledge of the heirs he has to destroy the letter. In the case of an electronic message the testator is free to delete or encrypt the message. In particular if the testator has not expressed such an intention, it is not the purpose of the rules on telecommunications secrecy to assume the role of an encryption device.

10.1.3 Conflict with Emerging Objectives of the Data Economy

The interpretation of the German rules on telecommunications secrecy by the KG Berlin is at odds with emerging legal principles and objectives of the data economy. The interpretation would make it impossible for the heirs to delete the data or the accounts of the testator. This would systematically lead to a surge of orphaned social media accounts and of orphaned personal data. The heirs and the next of kin would be prevented from deleting the accounts. The internet companies would have no authority to delete the accounts and also no interest to do so. As a consequence, the number of orphaned data and orphaned accounts would continually grow and they would de facto be attributed to the internet platforms, who could indefinitely exploit these assets.

Several arguments show that the emergence of orphaned personal data which are de facto and permanently attributed to an internet platform should be avoided and, as noted above,[97] that the de facto attribution of orphaned data to internet companies

[96] Herzog (2013), 3750.

[97] See 7.3.

would be contrary to the emerging legal policy principles of the data economy. The newly created rules on data portability[98] expressly seek to establish a right for users to retrieve their data from the internet platforms. Further, the current discussion about introducing an ownership right in data expressly does not seek to allocate such a right to the platform providers. Rather, it is the role and the autonomy of the data subject that is meant to be enforced. In addition, the postmortal right to personality is administered by the next of kin, who are in many cases identical with the heirs. Therefore, a deletion of the accounts or personal data should—as a default rule—rather be the task of the heirs and not of the internet companies.

10.1.4 The Need for Balancing Diverging Constitutional Rights

The KG Berlin in its decision invokes the constitutional basis of the rules on telecommunications secrecy. However, it is a well-established principle in constitutional law that the fundamental rights of all parties have to be respected to the highest degree possible. Accordingly, there should be a balancing between the secrecy of telecommunications on the one hand and other interests, which are also protected by constitutional law. For example, inheritance law has its constitutional basis in the right of property and, for example, entrepreneurial heirs have a constitutionally protected interest in continuing the business activities on electronic supply and sales platforms after the death of a business owner. Parents have a duty and a right to protect their minors from dangers. As part of their general right of personality parents have a right to be informed about the circumstances of their child's death. A mother is as a legal guardian under a legal obligation to control and supervise the online activities of her daughter. German courts have imposed quite strict supervision duties on parents and even ordered them to regularly study specialist articles in order to be better able to supervise their underage children's online behaviour.[99] It could, therefore, be argued that a person who sends an online message to an underage person could be presumed to have consented to the message being passed on to and read by the legal guardians.[100] In the concrete case the account of the deceased underage daughter was deactivated by an anonymous third party and there was a concern that the daughter's death could have been the result of a suicide. The sender of a possibly abusive message could not expect to be protected by the rules on telecommunications secrecy.

---

[98] See Article 20 Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/64/EC (General Data Protection Regulation).

[99] AG Bad Hersfeld, judgment of 20 March 2017 - F 111/17 EASO; AG Bad Hersfeld, judgment of 14 May 2017 - F 120/17 EASO.

[100] A general presumed consent not only for communications with minors is assumed by Steiner / Holzer (2015), 264. The KG Berlin rejects the idea of presumed consent arguing that many but not all minors would their access data on to their parents, see KG Berlin, judgment of 31 May 2017 - 21 U 9/16, 43.

In sum, the current German provisions on telecommunications secrecy in the TKG leave little room for the judges to undertake a balancing of diverging constitutional interests.

10.1.5 The Need to Adapt the Existing Provisions to Formerly Unknown Business Models

It has to be noted that the current German law on telecommunications secrecy and its exceptions have in essence been unchanged since 1996 and were not originally designed with regard to OTT services, which are a comparatively recent phenomenon. An explanation for the difficulties in applying this provision to OTT might be that there has been an asymmetry in extension of the provision by the courts. As noted above, with regard to the range of applicability there has been a threefold extension of the original provision by the courts. By contrast, the wording of the exceptions to the telecommunications secrecy leaves little room for interpretation and adaptation to OTT services. It would, therefore, be desirable for the legislature to clarify the role of telecommunications secrecy with regard to OTT services and, more specifically, with regard to the legal treatment of personal data after the data subject's death. The German Lawyers Association (Deutscher Anwaltverein, DAV) as early as 2013 presented a proposal to amend the German rules on telecommunications secrecy.[101] The proposed § 88 V TKG would stipulate an exception to telecommunications secrecy with regard to heirs.

10.2 Possible Features of a Holistic Approach

In a more general perspective on possible features of a holistic approach, it has to be noted that the legal treatment of personal data after the death of the testator is typically not governed by a single set of rules but is, rather, determined by various fields of law. The different fields of law pursue different objectives. Applying these rules to a particular scenario in a cumulative way guarantees that room is given to the different fields of law to bring effect to their objectives. Therefore, a holistic approach seeks to assure, at the outset, that the objectives of the respective field of law are and can be taken into account. Thereby, a basis is created for reconciling diverging concerns. Applying general rules of different fields of law to personal data constitutes an indirect regulation which incorporates different concerns. By contrast, applying only provisions of a single field of law would ignore the possibly legitimate aims of other fields of law. An isolated focus on one field of law would most likely be incomplete and not sufficiently take account of concerns which may be protected by other fields of law.

[101] Deutscher Anwaltsverein (2013), 6.

The provisions in the different fields of law will usually not have been specifically designed to be applied to a scenario where personal data are involved.[102] However, the exclusive application of a single provision to a case for which it has been specially created might in many instances fall short of reaching a satisfactory solution in the sense of a holistic approach. There is no single type of digital assets.[103] More generally speaking, there is, quite similarly, no single type of business model. The concern to make a new business model work needs to be balanced with other legal concerns affected. However, the weight to be attributed to making a business model work varies with regard to different business models and with regard to different legal concerns. In addition, two competing business models which serve the same purpose may affect legal concerns to a different degree. In some instances, it may be preferable not to put concerns aside and consequently not to allow a business model in order to uphold an incentive for the creation of a similar business model which impairs protected interests to a lesser degree. Conversely, the mere presence of personal data in a case scenario does not mean that the objectives of other fields of law can as a general rule be disregarded. In sum, it is quite unlikely that all different business models and such a wide range of differentiations can be captured in a single provision. Accordingly, a holistic approach does not necessarily imply that a single specifically tailored provision is or can be created or applied. Applying provisions from different fields of law may allow for a more nuanced differentiation than the application of a single specially tailored norm. Of course, if the satisfactory design of a single provision can be achieved, this would enhance legal security.

When applying provisions from different fields of law their objectives have to be identified. It needs to be examined whether the application of these provisions is required in order to attain their objectives in a scenario where personal data are involved. It should be avoided that a provision is applied even though its own objective would not require such an application. In such a case the provision would only be applicable by accident and might as an unintended consequence hinder the creation of a beneficial business model because the historic lawmakers did not have this kind of business model in mind. If the objective of a provision does not apply but, at the same time, the wording requires the provision's application, a review of the regulation by the lawmakers should be undertaken. For example, in the case discussed above, it would have to be examined whether the application of the provisions of telecommunications secrecy to OTT services actually intends to restrict the constitutional rights of heirs and of parents. Also, a harmonization with the rules regarding the analogue world, namely, with the secrecy of the post, should be examined more closely.

Also, the reverse situation can occur. The goal which a particular field of law seeks to achieve might be applicable in a particular scenario which involves personal data but the provision may not capture the case in question. In this instance the

[102] Alexander (2016), 307; Lange / Holtwiesche (2016b), 131.

[103] Berlee (2017), 256.

case at hand would by accident escape the application of a provision because the lawmakers did not have this particular new business model in mind. In this situation a revision of the provision by the courts or the lawmakers should be considered in order to avoid that the outcome of a case is determined by accident. In general, a legal reform should only be undertaken if a market failure has been detected.

More often than rarely the objectives of different fields of law might be in conflict with each other or with the concern not to create an unnecessary burden for new business models. In some cases it might be possible to identify provisions where the lawmakers—for example with regard to analogue cases—has already decided what weight is to be given to the conflicting concerns. In this event it has to be examined whether this decision can be transferred to a scenario which involves personal data or whether a special treatment is warranted because of the presence of personal data. For example, inheritance law clarifies that the privacy of a letter is no impediment for this letter to be handed over to the heirs. Similarly, the provisions on the secrecy of the post specify that this secrecy is no obstacle to the designation of a fiduciary who may receive the letters.

If there are not indications in existing law as to how to balance different legal concerns against each other, of course, the different objectives and the concern for privacy and the objective of not burdening new business models have to be balanced by the courts or by the legislature. Still, the inductive step-by-step procedure of a holistic approach may help to identify cases where a solution is to be found in an easier way and may, thereby, facilitate a learning process. Shortcomings and common features can be identified and as a possible synergy a specific approach taken in one field can inspire or complement a solution in other fields of law. Such a holistic approach will need time to evolve, as the scenarios which need to be considered are complex and of different character. Such a learning process would, in addition, be enriched by the analysis of cases from other jurisdictions and by a comparison of law.

References

Alexander, C. (2016), Digitaler Nachlass als Rechtsproblem, K&R 2016, 301

Berlee, A. (2017), Digital Inheritance in the Netherlands, EuCML 2017, 256

Bock, M. (2017), Juristische Implikationen des digitalen Nachlasses, AcP 2017, 370

Bräutigam, P. (2014), in: Burandt, W. / Rojahn, D. (Eds.), Erbrecht, 2nd ed., C.H. Beck

Chrobak, L. (2017), Digital Estate Revisited, Jusletter IT Flash 11 Dec 2017

Deutscher Anwaltverein (DAV) (2013), Stellungnahme Nr. 34/2013 zum Digitalen Nachlass, 52, available at: https://anwaltverein.de/files/anwaltverein.de/downloads/newsroom/stellungnahmen/2013/SN-DAV34-13.pdf

Deusch, F. (2016), Digitaler Nachlass – Vererbbarkeit von Nutzerkonten in sozialen Netzwerken, ZEV 2016, 189

Deusch, F. / Eggendorfer, T. (2007), Das Fernmeldegeheimnis im Spannungsfeld aktueller Kommunikationstechnologien, K&R 2007, 93

Drexl, J. (2017), Neue Regeln für die Europäische Datenwirtschaft?, NZKart 2017, 339

Fuchs, A. (2016), in: Ulmer, P. / Brandner, H. E. / Hensen, H.-D. (Eds.), AGB-Recht, § 307 para. 220, 12th edition, Dr. Otto Schmidt

Gebauer, J. (2015), Digitale Verlassenschaft, AkademikerVerlag
Gloser, S. (2015), "Digitale Vorsorge" in der notariellen Praxis, DNotZ 2015, 4
Gloser, S. (2016a), "Digitaler Erblasser" und "digitale Vorsorgefälle" – Herausforderungen der Online-Welt in der notariellen Praxis – Teil I, MittBayNot 2016, 12
Gloser, S. (2016b), Digitaler Nachlass, DNotZ 2016, 545
Graf von Westphalen, A. (2017), Nutzungsbedingungen von Facebook – Kollision mit europäischem und deutschem AGB-Recht, VuR 2017, 323
Harbinja, E. (2017), Digital Inheritance in the United Kingdom, EuCML 2017, 253
Herzog, S. (2016), Der digitale Nachlass ist in der Rechtswirklichkeit angekommen, ErbR 2016, 173
Herzog, S. (2013), Der digitale Nachlass – ein bisher kaum gesehenes und häufig missverstandenes Problem, NJW 2013, 3745
Hoeren, T. (2005), Der Tod und das Internet – Rechtliche Fragen zu Verwendung von E-Mail und WWW-Acounts nach dem Tode des Inhabers, NJW 2005, 2113
Klas, B. / Möhrke-Sobolewski, C. (2015), Digitaler Nachlass – Erbenschutz trotz Datenschutz, NJW 2015, 3473
Knoop, M. (2016), Digitaler Nachlass – Vererbbarkeit von Konten (minderjähriger) Nutzer in Sozialen Netzwerken, NZFam 2016, 966
Kuntz, W. (2016), Zugang der Erben zum Facebook-Nutzerkonto, FuR 2016, 398
Kunz, L. (2017), in: Staudinger Kommentar zum BGB, § 1922 para. 594 ff, 13th ed., Sellier - de Gruyter
Kutscher, A. (2015), Der digitale Nachlass, V&R unipress
Lange, K. W. / Holtwiesche, M. (2016a), Das digitale Erbe – eine rechtstatsächliche Bestandsaufnahme, ErbR 2016, 487
Lange, K. W. / Holtwiesche, M. (2016b), Digitaler Nachlass – eine Herausforderung für Wissenschaft und Praxis (Teil 1), ZErb 2016, 125
Leipold, D. (2017), in: Münchener Kommentar zum BGB, § 1922 para. 24 ff, 7th edition, C.H. Beck
Mackenrodt, M.-O. (2018), Digital Inheritance in Germany, EuCML 2018, 41
Maeschaelck, B. (2018), Digital Inheritance in Belgium, EuCML 2018, 37
Martini, M. (2015), Trauer 2.0 – Rechtsfragen digitaler Formen der Erinnerungskultur, GewArch Beilage WiVerw 2015, 35
Müller-Christmann, B. (2017), in: BeckOK BGB, § 1922 para. 99 ff, 42nd edition, C.H. Beck
Nemeth, K. / Carvalho, J. M. (2017), Digital Inheritance in the European Union, EuCML 2017, 253
Podszun, P. (2016), Rechtsnachfolge beim digitalen Nachlass, GWR 2016, 37
Preuß, N. (2017), in: BeckOGK BGB, § 1922 para. 347 ff., 375 ff., C.H. Beck
Raude, K. (2017), Der digitale Nachlass in der notariellen Praxis, RNotZ 2017, 17
Salomon, P. (2016), "Digitaler Nachlass" - Möglichkeiten der notariellen Vorsorge, NotBZ 2016, 324
Solmecke, C. / Köbrich, T. / Schmitt, R. (2015), Der digitale Nachlass – haben Erben einen Auskunftsanspruch? Überblick über den rechtssicheren Umgang mit den Daten von Verstorbenen, MMR 2015, 291
Seidler, K. (2015), Digitaler Nachlass, Wolfgang Metzner Verlag
Steiner, A. / Holzer, A. (2015), Praktische Empfehlungen zum digitalen Nachlass, ZEV 2015, 262
Stresemann, C. (2017), in: Münchener Kommentar zum BGB, § 90 para. 25, 7th edition, C.H. Beck
Wellenhofer, M. (2016), Erbrecht: Digitaler Nachlass, JuS 2016, 653
Wendehorst C. / Graf von Westphalen, A. (2016), Das Verhältnis zwischen Datenschutz-Grundverordnung und AGB-Recht, NJW 2016, 3745
Willems, C. (2016), Erben 2.0 – zur Beschränkung der Rechtsnachfolge in das "digitale Vermögen", ZfPW 2010, 494
Wurmnest, W. (2017), in: Münchener Kommentar zum BGB, § 307 para. 50, 7th edition, C.H. Beck
Zech, H. (2015), Industrie 4.0 – Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt, GRUR 2015, 1151

Additional Sources

AG Bad Hersfeld, judgment of 15 May 2017 - F 120/17 EASO
AG Bad Hersfeld, judgment of 20 March 2017 - F 111/17 EASO
BGH, judgment of 8 October 2013 - IX ZR 401/12
BGH, judgment announced for 12 July 2018 - III ZR 183/17
BVerfG 2, judgment of 16 June 2009 - BvR 902/06
Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 'A Digital Single Market Strategy for Europe' COM (2015) 192 final, 15
Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 'Building a European data economy' COM (2017) 9 final, 8
Directive (EEC) 93/13 of the Council of 5 April 1993 on unfair terms in consumer contracts OJ L95/29, 21 April 1993
KG Berlin, judgment of 31 May 2017 - 21 U 9/16
Law Commission UK (2017), Making a will, Consultation Paper 231
LG Berlin, judgment of 17 December 2015 - 20 O 175/15
Proposal for a Directive of the European Parliament and of the Council of 9 December 2015 on certain aspects concerning contracts for the supply of digital content COM(2015) 634 final
Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119/1, 4 May 2016 (GDPR)

The General Data Protection Regulation and Civil Liability

Emmanuela Truli

Contents

1 Introduction 304
1.1 Previous v. New Data-Protection Legal Framework 304
1.2 Examples of Data Breaches 307
2 Civil Claims According to the Repealed Data Protection Directive and Other Claims 309
2.1 Article 23 of Directive 95/46/EC and Its Transposing National Provisions 309
2.2 Other Tort Claims 314
2.3 Contract Breach Claims 316
2.4 Some Further Comments on Compensatory Claims 316
2.5 Requests for a Court Ruling 317
3 Civil Liability Under the New GDPR 318
3.1 Introductory Remarks 318
3.2 Material or Non-Material Damage 319
3.3 Liability of the Controller: Liability of the Processor 320
3.4 Joint Liability and the Right to Recourse 320
3.5 Persons Having the Right to Claim Damages 321
3.6 Presumption of Fault 322
3.7 Burden of Proof Regarding Infringement of the GDPR 323
3.8 Statute of Limitations and Other Procedural Rules 324
3.9 Other Effects of the GDPR 325
4 Conclusions 326
References 327

Abstract The General Data Protection Regulation (GDPR) took effect on 25 May 2018, on which date Directive 95/46/EC was repealed. The new GDPR has in some ways enhanced the protection of personal data: data subjects have expanded rights

Emmanuela Truli, *Dr. Juris* (LMU, Munich), *LL.M.* (Columbia, New York), Attorney at Law admitted in the Athens and New York Bar, is Assistant Professor of Civil Law at the Athens University for Economics and Business and a former Commissioner-Rapporteur of the Hellenic Competition Commission.

E. Truli (✉)
Athens University for Economics and Business, Athens, Greece
e-mail: etruli@aueb.gr

M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law*, MPI Studies on Intellectual Property and Competition Law 28, https://doi.org/10.1007/978-3-662-57646-5_12

and plaintiffs suffering harm for a data breach may file for restitution for their damage on the basis of the more comprehensive and coherent liability provision of Article 82. Many of the amendments and clarifications of this new provision are intended to (a) address the significant divergence in the liability rules transposing Article 23 of the repealed Data Protection Directive into national legislation and (b) complement such rules. These amendments are, mostly, very welcome, including: an explicit provision for compensation of moral damage, liability under certain conditions of the processor and joint liability of persons who have jointly caused the damage, and a right of representation of the data subject by a competent association.

1 Introduction

1.1 Previous v. New Data-Protection Legal Framework

European data-protection law was, until recently, governed by Directive 95/46/EC (the Data Protection Directive), which was supplemented by a few sectoral directives,[1] and had been transposed into national law[2] by all EU Member States as well as the European Economic Area (EEA) countries.[3] Since the enactment of Directive 95/46/EC,[4] there have been, however, considerable changes in the data-protection landscape: first, rapid technological developments of the past few years have increased the scale and importance of data collection and sharing, bringing about new challenges in the protection of personal data[5]; second, authorities have

[1] See e.g. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201/37 (Privacy and electronic communications Directive); Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105/54 (Retention of data Directive).

[2] It took a few years for the Member States to implement the Directive; see the European Commission's site on the Status of implementation of Directive 95/46: http://ec.europa.eu/justice/data-protection/law/status-implementation/index_en.htm. On the implementation and success of the Data Protection Directive see also Robinson / Graux / Botterman / Valeri (2009); Korff (2002); European Commission, Case No. COM/2003/0265 – First report on the implementation of the Data Protection Directive, 15 May 2003.

[3] European Economic Area: Iceland, Norway and Lichtenstein.

[4] For a general assessment of Directive 95/46/EC ten years after its enactment, see Poullet (2006).

[5] See European Commission, Proposal for a Regulation COM(2012) 11 final, 25 January 2012, SEC(2012) 72 final, SEC(2012) 73 final, Explanatory Memorandum, 1. See also Recital 6 of Regulation 2016/679/EU. On the new challenges to data protection see also the Comparative Study on different approaches to new privacy challenges in particular in the light of technological development, Final Report (2010) LRDP Kantor Ltd.

introduced information-exchange mechanisms between them in order to process data as part of the fight against transnational crime and terrorism, thus further enhancing the need for clear and consistent rules on data protection at EU level[6]; third, and closely connected to the above, awareness on the significance of personal data increased and the Lisbon Treaty introduced its protection as a fundamental right under EU law.[7]

It is, therefore, not surprising that the EU institutions considered an amendment of the Data Protection Directive, the process for which began as early as in 2009; after a public consultation, the Commission released a relevant Communication in late 2010.[8] Subsequently, all major participants in the process (the Council,[9] the Parliament,[10] the European Data Protection Supervisor,[11] and the Art. 29 Working Party[12]) published their views, both on the Commission Communication and with regard to their own standpoint on the possible amendments for the Directive.[13]

In April of 2016, the EU institutions finally concluded the reform package, which is comprised of: (a) the General Data Protection Regulation (EU) 2016/679 of 27 April 2016 (GDPR)[14] and (b) the Directive on the protection of personal

[6] See information on the webpage of the Council of the EU, available at: http://www.consilium.europa.eu/en/policies/data-protection-reform/.

[7] See Article 6(1) of the Treaty of the European Union, recognizing the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000 (as adapted in Strasbourg, on 12 December 2007), and Article 8 of the EU Charter of Fundamental Rights. See also Article 16 of the Treaty on the Functioning of the European Union and Article 8 of the European Convention on Human Rights.

[8] See European Commission, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - A comprehensive approach on personal data protection in the European Union, COM(2010) 609 final, 4 November 2010.

[9] See European Council, Council conclusions on the Communication from the Commission to the European Parliament and the Council – A comprehensive approach on personal data protection in the European Union, 3071st Justice and Home Affairs Council meeting Brussels, 24 and 25 February 2011.

[10] See European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Working Document (1 and 2) on a comprehensive approach on personal data protection in the European Union, 15 March 2011.

[11] See Opinion of 14 January 2011 on the Communication from the Commission on 'A comprehensive approach on personal data protection in the European Union'.

[12] See Letter from the Article 29 Working Party addressed to Vice-President Reding regarding the Article 29 WP's reaction to the Commission Communication 'A comprehensive approach to personal data protection in the EU', 14 January 2011.

[13] See De Hert / Papakonstantinou (2012), 130, 131 et seq.

[14] Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119/1, 4 May 2016 (GDPR).

data processed for the purpose of law enforcement,[15] or, as it is often called, the new Police and Criminal Justice Authorities Directive, aiming to establish a more efficient information-exchange mechanism between different judicial authorities.[16]

The GDPR took effect on 25 May 2018,[17] on which date Directive 95/46/EC was repealed,[18] whereby many (conflicting) provisions of national laws on the subject have been rendered inapplicable. It has been maintained that the release of a Regulation, rather than a new Directive, to replace the EU Data Protection Directive may have taken the data-protection community by surprise, but this critique is not justifiable, since the Commission in its Communication had enumerated emphatically the difficulties for EU data protection that were caused by the lack of harmonization among Member States.[19]

In any case, the GDPR declared as its aims, on the one hand, the provision of adequate protection to all EU member states citizens,[20] and on the other, the facilitation of businesses with the diminishing of undue administrative burdens.[21] Accordingly, a number of changes are introduced in the new data protection regime, including the express reference to the 'right to be forgotten',[22] provisions for easier access to one's data,[23] the right to know when one's data has been hacked,[24] rules for 'data protection by design and by default',[25] the abolition of the general notification

[15] Directive (EU) 2016/680 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/997/JHA, OJ L 119/89, 4 May 2016 (Police and Criminal Justice Data Protection Directive). The Directive must be transposed by member states by 6 May 2018.

[16] See European Commission, Press release (IP 16-1403), Joint Statement on the final adoption of the new EU rules for personal data protection, 14 April 2016. On the then pending data retention reform see also Robinson (2012), 394 et seq.

[17] See Art. 99 Regulation 2016/679.

[18] See Art. 94 Regulation 2016/679.

[19] See De Hert / Papakonstantinou (2012), 132 with further reference to Commission Communication, 2.2.

[20] See Recitals no. 10 et seq. and Article 1 of the GDPR.

[21] See Recital no. 9 and Article 1 of the GDPR. With regard to the effect of the new Regulation on businesses see e.g. European Commission (2016), Fact Sheet of January 2016, presenting benefits with regard to: facilitation of cross-border expansion, cutting of costs, creation of a level playing field, etc.

[22] See Recitals no. 65-66, 156 and Article 17 of the GDPR. See also ECJ, Google Spain and Google Inc. v. Agencia Espaňola et al, C-131/12, ECLI:EU:C:2014:317 and Kranenborg, *EDPL* 1/2015, 70.

[23] See Recital no. 39 and Article 15 of the GDPR.

[24] See Recitals no. 85-87 and Articles 30 and 31 of the GDPR. On the frequency of hacking, with numerous actual case from the US, see Foresman (2015), 344 et seq.

[25] See Recital no. 78 and Article 25 of the GDPR.

system[26] and its replacement with a 'data protection impact assessment',[27] increased fines for non-compliance,[28] etc.

1.2 Examples of Data Breaches

In today's information society personal data can be found in every organization, where it is maintained and managed for a wide variety of purposes (e.g. customer-relations management, HR management, service delivery, medical treatment, behavioral profiling etc.).[29] Central to the notion of personal data, and its need for protection, is, first and foremost, the data subject. A data subject is, according to the Data Protection Directive, any individual to whom the information relates, provided that he or she is identified or identifiable.[30] Looking at how this individual may be harmed, the following can be said: personal-data breaches may actually happen in numerous, currently conceivable and inconceivable situations. The personal-data subject may have willingly provided his personal information or this may have been attained by the data controller unlawfully; also, the data subject may be contractually connected to the data controller or not. In the interest of clarity, the above may be further illustrated as follows:

Example 1 A customer of an internet mail order company has been the subject of a security breach. All his information, including his credit card details, became freely available on the internet for almost 24 h, before the site was eventually taken down. He has had to freeze his credit card account and is worried that he may become the victim of identity fraud.[31]

Example 2 An individual's name is entered into an employee fraud database without justification. He accidentally finds out, is understandably distressed by the inference that he is a fraudster and requests the deletion of his name from the

[26] See Recital no. 89 of the GDPR.

[27] See Article 35 of the GDPR. The currently in force Data Protection Directive contains no provisions on impact assessments. The Directive provides for prior checking, which may be qualified as a forerunner of the data-protection impact-assessment requirement; arguably also Article 17 of the Directive could provide the legal basis for such an impact assessment; see on this subject and more on the data-protection impact-assessment novelty of the GDPR van Dijk / Geller / Rommetveit (2016), 287 et seq. For a possible definition of the term 'data protection impact assessment' see Wright / De Hert (2012), 5: 'a methodology for assessing the impacts on privacy of a project, policy, program, service, product or other initiative which involves the processing of personal information and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimize negative impacts'.

[28] See Recitals 148-152 and Article 82 of the GDPR.

[29] See i.e. Van Alsenoy (2012), 25.

[30] See Article 2(a) of the Data Protection Directive.

[31] See examples from the UK's data protection authority, available at: https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/compensation/.

list. There are two conceivable scenarios here: (a) the information about him is removed from the database before he applies for a new job and so he suffers no financial loss (pecuniary damage) as a result of the error, and only suffers distress; (b) the information about him is only removed after it has been accessed by a possible employer, thus preventing the individual from obtaining a job he has applied for.[32]

Example 3 An individual posts, on an internet platform she has signed up for, personal pictures and comments expressing her political views, on the basis of the agreement that the internet platform gives access to this information only to persons whom the individual has expressly selected. The internet platform accidentally makes all this information publicly available. The individual is fired from her job and/or is embarrassed about the fact that everybody has seen her personal pictures/political comments.

The individuals harmed by data breaches may, as a consequence, raise a damages claim for their emotional or financial harm, and/or they may request a court order so as to enforce their right e.g. to access their personal data, to prevent its processing or publication, and to rectify, block, or erase inaccurate personal data. Until recently, these legal actions were based either on the provisions transposing the Data Protection Directive in each (EU and EEA) Member State jurisdiction or on the general contractual and non-contractual national provisions. This paper shall, first, present the different civil measures (contractual and non-contractual, compensatory or not) that the harmed individual could take against the data controller or third parties under the repealed Data Protection Directive and, second, attempt to predict the effects of the new GDPR on the respective data-protection regime. Moreover, it is clarified that the analysis of potential claims arising from infringements of the e-commerce and the liability for the hosting of illegal content,[33] or the unfair contractual provisions legislation,[34] fall outside the scope of this particular work and require special attention.

[32] Ibid.

[33] 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, 17.7.2000, p. 1). Directive 2000/31/EC introduced special liability protection for hosting providers, namely no liability for services that 'consist of' the storage of electronic information, under the condition that the provider has no knowledge or awareness of illegal activity, and removes or blocks illegal data when it does gain knowledge or become aware of illegal activity ('notice and take down'), see Articles 12 to 15. Notably, the provisions of the GDPR are without prejudice to the application of the abovementioned rules of Directive 2000/31/EC; see Article 2(4) and Recital 21 of the GDPR. On the interaction between e-commerce provisions and data-protection rules see also Sartor (2013), 4 et seq.

[34] See Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ L 95, 21.4.1993, p. 29).

2 Civil Claims According to the Repealed Data Protection Directive and Other Claims

2.1 Article 23 of Directive 95/46/EC and Its Transposing National Provisions

Directive 95/46/EC required Member States to introduce a provision awarding data subjects a judicial remedy, especially against data controllers.[35] More particularly, Article 23 ('Liability') stated:

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.
2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

This was evidently a non-contractual/tort provision, in the sense that it did not require that the person who has suffered damage from a data breach have a contractual relationship with the responsible controller; hence also its transposed national rules related to a tort claim, and there could be no requirement for a contract breach between the data controller and the data subject for a respective claim before national courts.

2.1.1 Persons Having a Right to Claim Damages

Following the above understanding (of a non-contractual/tort claim) and with regard to the possible claimants, Article 23 of the Data Protection Directive appeared to allow claims from **any** person who had suffered damage as a result of a data breach, theoretically, then, also from a person *other* than the one whose personal information has been misused.[36] Such a case could arise when personal data of one person have been made public unlawfully, but this data-processing breach (also) causes harm to another person: for example when there is unlawful data breach regarding DNA information of one or both parents, revealing personal information about their child. In this example, if all other requirements of liability (such as damage[37] and

[35] See also Recital 55 of Directive 95/46/EC.

[36] See also Christodoulou (2013), para. 232 and the decision of the Athens First Instance Court 2516/2004, *DiMEE* 2006, 74. See, however, Kanellopoulou-Mboti (2016), 416, with references to the two Greek court decisions 1257/2005 Athens Court of Appeals, *Nomiko Vima* 205, 289 and 1434/2005 Athens First Instance Court, *DiMEE* 2005, 75.

[37] See in this respect the Irish case about Section 7 of the Irish Data Protection Acts 1988 and 2003 (Irish DPA) *Collins v. FBD Insurances*, where the court confirmed that the transposed provision did not give rise to an automatic right to compensation in the absence of evidence of actual loss or damage.

fault of the data controller) were met, the person having suffered damage could be able to claim compensation on the basis of the national provisions transposing Article 23 of the Data Protection Directive, irrespective of the fact that the data breach concerned another data subject's information. This, however, may not always have been the case. In Germany, for example, § 7 of the Federal Data Protection Act (*Bundesdatenschutzgesetz*—BDSG)[38] seems to have limited the possible claimants to persons who have suffered harm from the breach of their own personal data, thus excluding claims from third persons.[39]

In addition, Article 23 of the Data Protection Directive did not necessarily exclude claims from legal persons. More specifically, a legal person could conceivably suffer damage due to a breach of the data-protection rules in relation to a natural person's data. In this case, and according to the wording of Article 23 of the Data Protection Directive, the legal person could probably raise a claim against the controller, and receive compensation, provided, of course, all other requirements were met. This was, however, not always clear with regard to the transposed national provisions. In Germany, for example, courts have not ruled on the subject and the prevailing view in legal theory seemed to exclude such possibility on the basis of the argument that the Data Protection Directive aimed at the protection of natural persons only.[40] This argument was not very convincing, since it did not take into account that any sanctioning of data breaches also has a preventive effect.[41] Arguably, to the extent that the scope of the national transposing provisions has been limited in the above manner in one or more jurisdictions, this could have been a case of suboptimal transposition of Article 23 of the Data Protection Directive.

2.1.2 The Person Responsible for Damages

The claim according to Article 23 of Directive 95/46/EC was filed against the data controller. The 'controller' according to Article 2(d) was defined as 'the natural or legal person, public authority, agency or any other body which alone or jointly with

[38] See the text in the original: 'Fügt eine verantwortliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist sie oder ihr Träger dem Betroffenen zum Schadensersatz verpflichtet. Die Ersatzpflicht entfällt, soweit die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.'

[39] See BeckOK DatenSR/Quaas (2013), BDSG § 7, para. 7. See also the decision of *Bundesarbeitsgericht* which stated that the employer does not have a claim against the union of workers for the sending of advertisement e-mails sent to the business addresses of his employees, because these are considered personal data of the latter, BAG NJW 2009, 1990.

[40] Ibid., para. 7.1. See also ibid., para. 35 et seq.

[41] The introduction of a risk of civil liability seeks to ensure that any damage caused by unlawful processing receives appropriate compensation: see Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of 'controller' and 'processor', WP169, 16 February 2010, 5. The German jurisprudence at times overlooks the preventive nature of damages: see BeckOK DatenSR/Quaas (2013), BDSG § 7 para. 2.

others determines the purposes and means of the processing of personal data'. Notably, and in view of the fact that entities often, in practice, outsource some of these operations to other entities hired to manage personal data on their behalf, Directive 94/46/EC also provided a definition of the 'processor', as the 'natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller'.[42] The processor was, according to the Data Protection Directive, not liable for the data breach; it was only the controller who was responsible—and also for the data breaches of the processor.[43] Hence, the qualification of an entity as either a controller or a processor had significant implications in terms of the allocation of liability.[44] The Directive was criticized for not providing for joint liability of the two or an exemption from this rule, as it is conceivable that the processor could exceed his/her mandate and not follow the instructions of the controller, in which case it would seem more justified that the former should be liable, instead of the controller.[45]

Interestingly, the Data Protection Directive provided no time-limitation (prescription) for the damages claim against the controller. It may well be expected that in most jurisdictions no such provision would be included in the transposing data-protection act. Since, however, the prescription rules are a general principle of civil-liability law across jurisdictions, one may presume that the national provisions transposing Article 23 of the Data Protection Directive were also subject to the general-limitation provision applicable in the national legislations for tort actions.[46]

2.1.3 Breach, Causality and Fault

Article 23 of the Data Protection Directive and its transposed national rules should have applied only when there is a data breach, namely, a breach of the Directive rules about the conditions for the lawful processing of personal data. Examples of such data breaches are the following: collection of personal data for unlawful purposes, collection of personal data without consent of the data subject, where no

[42] See Article 2(e) of the (repealed) Data Protection Directive.

[43] The contractual agreements between them could therefore provide for a 'liability sharing' clause, determining who will ultimately bear the cost of compensation; see BeckOK DatenSR/Quaas (2013), BDSG § 7 para. 40. If such clause is missing, the national breach-of-contract provisions will apply and liability shall be shared according to the respective rules of each jurisdiction. Hence, processors are, as a rule, only indirectly liable for compliance obligations under Directive 95/46/EC.

[44] And also for the determination of the law applicable and the responsibility to comply with the substantive provisions of the Data Protection Directive, see also Van Alsenoy (2012), 26. For guidance on how to apply the concepts of controller and processor see the opinion of the Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of 'controller' and 'processor', WP169, 16 February 2010.

[45] Thus for Germany; see indicatively BeckOK DatenSR/Quaas (2013), BDSG § 7 para. 41.

[46] Thus for Germany; see Gola / Klug / Körffer (2015), BDSG § 7 para. 20.

exception to the requirement of consent exists, processing of data without a necessary notification to the data-protection authority, dissemination and use of the data without the data subject's consent, storing or dissemination of false data, etc.

The Directive did not seem to provide for a presumption against the controller in terms of causality: it may therefore be presumed that in most transposing provisions no such assistance to the claimant had been introduced either, and that the latter would bear the burden of proving that the data breach was directly connected in terms of causation with his or her damage.[47] This may in practice have presented difficulties, since the person who has suffered damage may not easily have had access to information proving that e.g. he did not get a job offer or credit due to the incorrect information collected, stored or disseminated by the controller,[48] or the damage may not have been immediate.[49] In any case, national courts applied their own internal rules for the requirement of causation.

With regard to fault, however, Article 23(2) stipulated that 'the controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage'. This provision clearly indicated that the controller's fault was presumed in case of a data breach.[50] The controller could, nevertheless, be exempted from his liability if he contended and proved that he took all necessary precautions, and was not negligent with regard to or intended the event giving rise to the damage. Differences between Member States seem to have existed here as well. For example, in Belgium and Portugal the controller was liable for compensation unless he proved that he was not responsible for the event that caused the damage; in Denmark, on the other hand, the law provided that the controller is liable for 'any damage caused by the processing of data in violation of the provisions of this Act, unless it is established that such damages could not have been averted through the diligence and care required in connection with the processing of data'.[51] In Finland, France, and Luxemburg the ordinary rules on civil liability applied.[52] Jurisdictions transposing Article 23 into national law in this way, hence, were also bound to connect its application with the national understanding of fault.[53]

---

[47] Thus in Germany; ibid., para. 7.

[48] See also ErfK/Franzen(2016), BDSG § 7 para. 1. For a German case in which the claimant failed to prove the causation between his damage and the data breach, see LG Bonn NJW-RR 1994, 1392.

[49] See also Clifford / Van Der Sype (2016), 277 et seq. On the difficulties of proving causation and damage see also: European Union Agency for Fundamental Rights (2013), Access to data protection remedies in EU Member States, 28 et seq.

[50] See for Germany indicatively Gola / Klug / Körffer (2015), BDSG § 7 para. 9.

[51] See Korff (2002), 179 et seq.

[52] Ibid., 180.

[53] See e.g. the German approach, which takes into consideration the expected standard of care under the particular circumstances, whereby the more sensitive the information the higher is the standard of care and the existence of certification and quality-control mechanisms may also be taken into account; see BeckOK DatenSR/Quaas (2013), BDSG § 7 para. 63 et seq.

In any case, it is worth noting that the respective wording of Article 23(2) was arguably a bit unfortunate. A reading of the sentence that the controller 'may be exempted from this liability, in **whole or in part,** if he proves that he is not responsible for the event giving rise to the damage' (emphasis added) could conceivably suggest that the controller may actually sometimes have exculpated himself only partly, even though 'he is not responsible for the event giving rise to the damage'. According to this (incorrect) reading, a judge could both have recognized that the controller was not liable for the event giving rise to the damage and have exculpated him only partly. Of course, this reading is evidently incorrect. If read correctly, this sentence simply stipulates that a court could have allocated only part of the liability to the controller: to the extent that he could exculpate himself for part of the responsibility, he would also only be partially responsible for the damage.

2.1.4 The Requirement for Material Damage (?)

Member States have transcribed this provision into their national laws, but, in view of the fact that the Directive did not further define the notion of 'damage', not always in the same manner. Greece, for example, implemented the Directive provision by way of Article 23 of Law 2472/1997, which provided for compensation of any damage, namely (and expressly), also immaterial or moral damage from data breaches.[54] Germany, on the other hand, implemented the liability provision of Directive 95/46/EC in § 7 of the BDSG following the example of the Directive's general reference to damage, but seems to have applied it only when there was material damage or pecuniary loss, thus not when there was just moral damage.[55]

The restitution of only moral damage seems to have been questionable also in other jurisdictions, such as the UK. Section 13(1) of the Data Protection Act 1998 provided an individual with a right to compensation for damages for breach of the DPA, and Section 13(2) stated that an individual who suffers distress arising from a breach of the Act is entitled to compensation only if the individual 'also suffers damage' (or the processing is for 'special purposes': journalistic, literary or artistic purposes): this damage

[54] See Article 23 L. 2472/1997: '1. Any natural person or legal entity of private law, who in breach of this law, causes material damage shall be liable for damages in full. If the same causes non pecuniary damage, s/he shall be liable for compensation. Liability subsists even when said person or entity should have known that such damage could be brought about. 2. The compensation payable according to article 932 of the Civil Code for non pecuniary damage caused in breach of this law is hereby set at the amount of at least two million Drachmas (GRD 2,000,000), unless the plaintiff claims a lesser amount or the said breach was due to negligence. Such compensation shall be awarded irrespective of the claim for damages.' On the Greek Data Protection Law see also Mitrou (2010), Country Studies, A.5. Greece, 3 et seq.

[55] See Gola / Klug / Körffer (2015), BDSG § 7 para. 12; BeckOK DatenSR/Quaas (2013), BDSG § 7 para. 55 with further references, indicatively to Tremml / Karger / Luber (2013), para. 1047; references to the opposing opinion include Wächter (2014), para. 1053, and Scheja / Haag (2013), 5 para. 366.

had previously been interpreted as meaning pecuniary loss.[56] This has, however, clearly changed in the *Vidal-Hall* case, where three British individuals claimed that Google collected private information about their internet usage via their Apple Safari browser without their knowledge or consent, and then made such information available as part of its commercial offering to advertisers.[57] The claimants sought damages for anxiety and distress, but did not make any claim for pecuniary loss. The Court of Appeal confirmed that claimants can claim compensation for distress without having to prove pecuniary loss.[58] The Court of Appeal held in particular that '[s]ince what the [Data Protection] Directive purports to protect is privacy rather than economic rights, it would be strange if the Directive could not compensate those individuals whose data privacy had been invaded by a data controller so as to cause them emotional distress (but not pecuniary damage)'; finding that this would be incompatible with the right to an effective remedy under Article 47 of the EU Charter of Fundamental Rights, the court thus requested the disapplication of Section 13(2) of the UK Data Protection Act.[59]

2.2 Other Tort Claims

Breaches of the national data-protection rules can result to damages claims on the basis of the general tort provisions in most, if not all, of the EU (and EEA) Member State jurisdictions. The requirements for such claims are national, but they should

[56] See Palmer (2015); further explaining that the need for claimants to prove pecuniary loss as a prerequisite to claiming for distress has required significant evidential contortions in the past, see e.g. *Johnson v MDU* [2006] EWHC 321. In this case the claimant had brought an action against his old insurer for compensation under Section 13 of the Data Protection Act 1998 for unfair processing of his personal data. The claimant contended that he had a case against the risk manager who prepared materials for consideration by the risk management group: he had purportedly unfairly selected them, which led to termination of the claimant's insurance coverage and great damage to his professional reputation. The Court held that the preparation of a summary by the risk manager was processing according to Section 1(1) of the DPA 1998 but that the unfair processing element had not caused the mutual society to terminate the claimant's membership.

[57] See *Vidal-Hall v Google Inc,* [2014] EWHC 13 (QB), Judgment of 16 January 2014.

[58] Interestingly, the Court of Appeals also decided that browser-generated information (BGI) such as cookies constitute 'personal data'. Google argued that BGI was anonymous information. The Court of Appeals examined first whether the BGI identified an individual by itself: on the basis of the Opinion issued by the Working Party 29 on the concept of personal data and the decision of the European Court of Justice in *Lindqvist*, the court stated that the correct approach may be to consider whether the data 'individuates' the individual (differentiates him from others) and that it is not necessary for the data to reveal information such as the actual name of the individual. Since the BGI told Google such information as the claimants' unique IP address, the websites they were visiting, and even their rough geographic location, the Court of Appeal concluded that it is likely that the individuals were sufficiently individuated and that the BGI on its own constitutes 'personal data'. See also Palmer (2015).

[59] See para. 91 et seq. in the decision *Vidal-Hall v Google Inc*, [2014] EWHC 13 (QB); see also the court's referral to the ECJ, *Leitner v. TUI Deutschland Gmbh & Co KG*, C-168/00, ECLI:EU:C:2002:163.

probably be closely connected to the notion of the data breach, namely, the infringement of the collection and processing rules prescribed in the national data-protection legislation,[60] which enacted the Data Protection Directive in each Member State.

In some jurisdictions, however, additional, specific, non-contractual provisions may also be applicable, for example, provisions protective of the right to the individual's personality. Such is the case in France and Greece, the Civil Codes of which include special provisions against infringements of the 'right to one's private life'[61] or the 'right to one's personality'.[62] Notably, the German jurisprudence has also recognized the protection of the right to one's personality, as a specific tort.[63] Under such personality-specific claims, the claimant usually has to prove the infringement to his or her right to personality (which has been caused by the infringement of the rules of the respective national data-protection act) and that the other conditions for a tort claim are met. Obviously, in such cases, there is no reversal of the burden of proof, for example in the requirement of fault, as would be the case if the claim were based on the national provisions transposing Article 23 of the repealed Data Protection Directive.[64] Moreover, these rules are applicable not only against the data controller (as in Article 23), but also against any other tortfeasor or person infringing the right to one's personality. For example, in the case that hit the news a short while ago about Pippa Middleton's pictures being stolen from her cloud account, Ms Middleton could potentially have a claim against the cloud services provider/data controller, but certainly also a claim against the hacker of her account. The claim against the data controller could have been based on the national provision transposing Article 23 of the repealed Data Protection Directive, if all the conditions thereof are satisfied. Against the hacker, however, she would also have a general tort claim (or a claim for the infringement of the right to her personality, to the extent such claim existed in the UK).

Finally, some jurisdictions, like Greece and Germany, have recognized a claim for pre-contractual liability (for acts executed during negotiations—*culpa in contrahendo*).[65] This is a non-contractual liability claim, related to the negligent or intentional breach of the duty of care (trust) during the process of negotiations.

---

[60] This is at times also sanctioned with criminal penalties. Criminal provisions are in some jurisdictions, such as Greece, considered to have the object of protecting the individual, hence can be used in conjunction with the general tort provisions for the substantiation of tort claims (namely with Article 914 of the Greece Civil Code).

[61] See Article 9 of the French Civil Code, Loi 1803-03-08 (as amended and currently in force): 'Chacun a droit au respect de sa vie privée. Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée: ces mesures peuvent, s'il y a urgence, être ordonnées en référé.'

[62] See Article 57 of the Greek Civil Code. See also Christodoulou (2013), para. 224.

[63] The Federal Protection Act (BDSG) is considered a 'protective provision' as required by § 823(2) of the German Civil Code (BGB).

[64] See indicatively for Germany ErfK/Franzen (2016), BDSG § 7 para. 1; BeckOK DatenSR/Quaas (2013), BDSG § 7 para. 1.

[65] See indicatively Articles 197-198 of the Greek Civil Code.

A pre-contractual liability in relation to a data breach may be recognized e.g. when the data subject provides personal data to another person within the framework of a process of negotiation for the conclusion of a contract.[66]

2.3 Contract Breach Claims

In many instances, however, the controller will indeed have entered into a contractual relationship with the data subject. Examples 1 and 3 mentioned above relate to such cases. The case of Pippa Middleton's pictures is also a possible example: Ms Middleton entered into a contractual agreement with a cloud service provider; to the extent that her service provider/data controller is responsible for the data breach (e.g. because it had the obligation to protect her data and negligently failed to take all necessary measures to that end) it could have been liable (not only on the basis of the national provision transposing Article 23 of the repealed Data Protection Directive, but also) on the basis of the general breach-of-contract provisions (and its conditions) of the respective jurisdiction.

In most instances the person entitled to claim damages according to the breach-of-contract rules will be the data subject itself. This may not, however, always be the case. It is conceivable that the data breach (e.g. the stolen or otherwise wrongful information) will harm a third person other than the data subject (or both the data subject and a third person). For example, there is the case of a credit information service providing to a bank, on a contractual basis, credit information on persons who submit loan applications to the bank. Due to an inaccurate credit listing about a particular person (who was not creditworthy), the bank provides the credit. The loan servicing stops and the bank suffers financial loss. In this case, the inaccurate listing has caused damage to the bank and not the data subject itself (who in fact has benefited from the inaccurate credit-listing information in the sense that he acquired the credit he requested).

2.4 Some Further Comments on Compensatory Claims

All these (contractual and non-contractual) claims are, of course, not mutually exclusive.[67] In that respect, in Example 1, if the hacking of personal data (credit card information) of a particular person resulted in harm of that person and assuming that the target of the hacking was negligent, there is a plethora of possible claims: the data subject had a contract-breach claim against the internet mail order company and a claim based on the national provision transposing Article 23 of the repealed Data Protection Directive against the data controller (the mail order company). Obviously, both the data subject and the internet mail order company have a tort claim against the hacker of the stolen credit card information.

[66] See indicatively for Germany Gola / Klug / Körffer (2015), BDSG § 7 para. 18.

[67] See for Germany indicatively Gola / Klug / Körffer (2015), BDSG § 7 para. 16.

In addition to any of the above claims, in a number of jurisdictions, such as Germany and Greece, the successful claimant in a court proceeding also has a claim for his court and attorney costs.[68]

Moreover, in many jurisdictions there are joint and several liability rules; these are applicable whenever the damage has ensued following the data breaches of more than one data controller, where, for example, data is collected unlawfully by one data controller, and following its transfer, is again unlawfully processed by another data controller.[69] However, these rules were, most probably, inapplicable to claims based on national provisions transposing Article 23 of the repealed Data Protection Directive, as its paragraph 2 (on the possibility of partial exculpation of the controller) could not be readily reconciled with the joint and several liability mechanism.[70]

Finally, in any of these claims (again, contractual and non-contractual), the data breach may be attributable to intent (and not negligence): many data breaches are intentional, often due to the substantial economic benefits that the controller may gain from the unlawful use of the personal data: one only has to think of a hospital providing patients' information[71] to group companies or third companies for purposes of direct marketing, or a cloud-services provider, secretly going through stored documents of data subjects[72] for the same reason.

2.5 Requests for a Court Ruling

Although at times a person suffering damage from a data breach may request compensation, in other instances one may primarily needed to prevent or stop an infringement of the repealed Data Protection Directive rules (as these were transposed in national provisions) before any harm (or more harm) ensued. Of course, at other times, a person may have needed to request all of the above, namely, both compensation and a court order/injunction relief against the data controller and/or a third person.

With regard to the content of the request for an injunction relief, this could seek to order the data controller to comply with any of the data subject's rights following

---

[68] See for Germany BeckOK DatenSR/Quaas (2013), BDSG § 7 para. 4 with reference to the case OLG Zweibrücken, Decision of 21.2.2013 – 6 U 21/12, JAmt 2013, 414.

[69] Thus in Germany see Gola / Klug / Körffer (2015), BDSG § 7 para. 15.

[70] See above, under 2.1.3. Compare also below, under 3.4.

[71] Especially for patient personal data see also Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45) and in particular Article 4(2)(f)): 'in order to ensure continuity of care, patients who have received treatment are entitled to a written or electronic medical record of such treatment, and access to at least a copy of this record in conformity with and subject to national measures implementing Union provisions on the protection of personal data, in particular Directives 95/46/EC and 2002/58/EC'.

[72] This may be the case for some cloud-services providers: see Stylianou / Venturini / Zingales (2015), 11 et seq. On the cases of a number of EU Data Protection Authorities against Google see Voss (2014/2015). On the notion of cloud computing and its privacy risks see also Svantesson / Clarke (2010), 391 et seq.

the repealed Data Protection Directive, as this was transposed into national legislation. For example, in the UK,[73] the court could order a data controller to comply with a data subject's: (a) right to access one's personal data,[74] (b) right to prevent processing of personal data likely to cause damage or distress,[75] (c) right to prevent processing for purposes of direct marketing,[76] and (d) rights in relation to automated decision-making.[77] The court could also order the rectification, blocking, erasure, and destruction of inaccurate personal data.[78]

In Germany, where non-contractual claims for breaches of data-protection rules were rare, the harmed party usually requested an injunction relief for rectification, erasure, and blocking of the personal data, according to §§ 6, 20 and 35 of the previous BDSG.[79] Requests for a cease-and-desist order may be based on national rules, sometimes also on the basis of non-contractual claims (tort or personality-protection rules).[80]

3 Civil Liability Under the New GDPR

3.1 Introductory Remarks

The new GDPR took effect on 25 May 2018.[81] On that date, Directive 95/46/EC was repealed,[82] and all the Member State provisions transposing the Data Protection Directive into national legislation became, to the extent that they conflicted with the

[73] See Franet Contractor, Ad Hoc Information Report, Data Protection: Redress mechanisms and their use, United Kingdom (2012), University of Nottingham Human Rights Law Centre.

[74] See Section 7 of the UK Data Protection Act.

[75] See Section 10 of the UK Data Protection Act. See also the 2011 High Court case *Law Society v. Kordowski* [2011] EWHC 3184 (QB), which held that the defendant's processing on his website of the claimant's personal data was in breach of the data-protection principles. A perpetual injunction under Section 10 of the UK Data Protection Act (prevention of data processing) was granted, ordering the defendant to cease processing the claimant's personal data.

[76] See Section 11 of the UK Data Protection Act.

[77] See Section 12 of the UK Data Protection Act.

[78] See Section 14 of the UK Data Protection Act. In the case *Law Society v. Kordowski* [2011] EWHC 3184 (QB) mentioned above, the court also issued an order under Section 14 of the UK Data Protection Act requiring the defendant to block, erase, and destroy all the data that was the subject of the claim.

[79] See BeckOK DatenSR/Quaas (2013), BDSG § 7 para. 3.

[80] For Germany see indicatively ibid., § 11 and 11.1. See, however, BAG NJW 2009, 1990, 1996 with reference to a desist order on the basis of the application of § 7.

[81] See art. 99 of Regulation 2016/679.

[82] See art. 94 of Regulation 2016/679. See also Recital 171 of the Regulation, which further explains that 'processing already under way on the date of application of this Regulation should be brought into conformity with this Regulation within the period of two years after which this Regulation enters into force. Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which

Regulation, immediately inapplicable. Member States should have timely abolished the respective provisions in their national data-protection acts, so as to avoid the confusion and uncertainty to be caused to lawyers, judges, controllers, data subjects and the public, by the concurrent existence of conflicting legislative frameworks (the national one and that of the GDPR).[83] In addition, Member States may have needed to introduce some new national provisions in order to comply with some of the GDPR provisions and in order to establish their preferred options of those presented in the Regulation.[84] As regards the question of whether national provisions, which potentially provide a higher level of data protection, can remain applicable in parallel to the GDPR, the answer may be twofold: Member States may pick their own option, as long as the Regulation provides them with such an opportunity; when no options for diverging rules are provided in the GDPR text, it may be safely presumed that, given the aim of the Regulation to introduce a harmonized level of protection across the EU,[85] such diverging/higher protection rules, can no longer continue to exist.

In any case, the GDPR introduced one distinct civil-claim provision for data-breach liability, which does not seem to permit deviations between Member States. Article 82 of the GDPR has the title 'Right to compensation and liability' and is comprised of six paragraphs (four more than the two provisions in the repealed Data Protection Directive), introducing a more comprehensive system of liability. Interestingly, the additions and amendments of the new GDPR civil-liability provision seem to directly address some of the difficulties of the divergent national rules highlighted above.

3.2 Material or Non-Material Damage

More particularly, the GDPR clarifies right from the start that compensation is possible for any kind of damage: either pecuniary or moral. Article 82(1) stipulates, namely, unequivocally that '1. Any person who has suffered **material or non-material damage** as a result of an infringement of this Regulation shall have the

---

the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation. Commission decisions adopted and authorizations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed'.

[83] See also Eickelpasch (2016), 22 favoring an amendment of the national provisions of the German Data Protection Act (and the federal state laws) that are in conflict with the GDPR rules.

[84] Critical on the many options of the GDPR which provide large room for maneuver in the Member States and their data-protection authorities, see Piltz (2016), 557. Considering that, in this respect, the GDPR is an '*atypical hybrid between Regulation and Directive*', see Kühling / Martini (2016), 449.

[85] See also Piltz (2016), 560 and the document of the Council 14732/14 of 24.10.2014, available at: http://data.consilium.europa.eu/doc/document/ST-14732-2014-INIT/en/pdf on the proposal of a 'minimum harmonization' clause (Article 1 para. 2a proposed by the Council), which would allow the Member States to introduce higher protection rules, and which was not included in the final text.

right to receive compensation' (emphasis added). This clarification is very welcome and puts to rest any diverging opinions and national approaches with regard to moral damage, which is now clearly included in the notion of damage and must be compensated when it ensues from a data breach.

3.3 Liability of the Controller: Liability of the Processor

The first paragraph of Article 82 GDPR offers one more amenable change: the party obligated for restitution of the damage may not only be the controller, but possibly also the processor. Article 82(2) goes on to explain that it is principally the 'controller involved in processing' who 'shall be liable for the damage caused by processing which infringes this Regulation'; nevertheless, a 'processor shall be liable for the damage caused by processing where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller'. It is therefore clear that the processor is no longer immune from liability and the data controller is not the only person who may be liable for compensation in case of a data breach. This amendment answers the criticism that it does an injustice to the controller if the processor exceeds his mandate or does not follow his orders,[86] and somewhat limits the importance of the qualification of an entity as either a controller or a processor, for the allocation of liability.[87]

3.4 Joint Liability and the Right to Recourse

The claim for restitution must, hence, be addressed against the person responsible for the data breach: this person **may be either the controller(s)**[88] **or the processor(s); also, they may be one or more of both.** Article 82(4), namely, explains that '[w]here more than one controller or processor, or **both** a controller and a processor are involved in the same processing and where they are […] responsible for any damage caused by processing, each controller or processor shall be held liable' (emphasis added). In fact, the same provision further explains that in this case, the above persons are responsible 'for the entire damage'. Hence, the GDPR introduces the principle of **joint liability** of all persons accountable for the damage.

[86] For Germany, see indicatively BeckOK DatenSR/Quaas (2013), BDSG § 7 para. 41. Although, of course, in practice, the controller and processor could allocate liability between them on the basis of their contractual agreements.

[87] See also Van Alsenoy (2012), 26.

[88] See also Article 26 of the GDPD about 'joint controllers'.

As already mentioned above, the notion of joint liability is standard for joint tortfeasors in many jurisdictions, including Germany[89] and Greece.[90] Nevertheless, it seems that joint liability was incompatible with the claims based on the provisions which transposed Article 23 of the repealed Data Protection Directive into national legislation. This was due to the fact that Article 23(2) of the repealed Data Protection Directive stipulated that the controller could 'be exempted from this liability, **in whole or in part,** if he proves that he is not responsible for the event giving rise to the damage' (emphasis added). As already indicated above (under Sect. 2.1.3.) the correct reading of this provision related to the partial exculpation of the controller when he was only partially liable for the damage, which could not be reconciled with a joint-liability clause.

In any case, the GDPR now introduces the principle of joint liability across the EU, which is useful in terms of both the protection of the person who suffered the damage and the uniform application of Article 82. On the same note, Article 82(5) further explains that '[w]here a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, **that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing** that part of the compensation corresponding to their part of responsibility for the damage' (emphasis added). This is again a standard stipulation within the joint-liability mechanism, the usefulness of which extends from only ensuring that there is no respective uncertainty (in relation to jurisdictions which already follow this rule), to the innovative introduction of the recourse mechanism in relation to any jurisdictions not already having such rule.

Finally, the provision explains that recourse shall apply 'in accordance with the conditions set out in paragraph 2'. This, as already explained, stipulates:

> Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

Hence, it will be a matter of fact, for the judge, to allocate liability, and to establish to what extent each of the involved actors (processors/controllers) is responsible for the data breach (the percentage of the defendants' liability)—all in all a challenging exercise.

3.5 Persons Having the Right to Claim Damages

Although Article 82(1) clearly stipulates that '[a]ny person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation', a less amenable change in the wording and,

[89] See §§ 830 and 840 BGB. See also § 421 BGB.

[90] See Articles 926-927 of the Greek Civil Code. See also Article 481 Greek Civil Code.

as a consequence, possibly the scope of the GDPR liability clause, is included in Article 82(4). As previously analyzed, this provision primarily aims at introducing the joint-liability rules when more than one person is accountable for the incurred injury. The provision hence stipulates, first, that 'each controller or processor shall be held liable for the entire damage' and, then continues to explain that this should be so **'in order to ensure effective compensation of the data subject**'. This wording is particularly unfortunate, as it will most certainly affect the discussion on the scope of the GDPR liability clause. Under the liability rule of the repealed Data Protection Directive, no reference existed which would limit the persons having standing for a claim against the data controller to the data subject. Instead, as indicated above, it was conceivable that a third person could also suffer damage from the controller's actions with regard to another person's data and that this third person should have standing to sue on the basis of the national provisions implementing the repealed Data Protection Directive. Following the coming into force of the GDPR, the respective position is seriously weakened by the unfortunate reference of Article 82(4). It is, therefore, possible that national courts will deny the protection of Article 82 to third persons, despite the fact that the particular reference is most probably accidental. Notably, should the Community legislature have intended to actually limit the scope of Article 82, it could have easily done so by including this wording in its first paragraph. By way of a reminder, the wording there pronounces that '[a]ny person who has suffered […] damage as a result of an infringement of this Regulation shall have the right to receive compensation' without referring to 'any data subject who has suffered damage'. Unfortunately, now courts in Member States may take divergent stances with regard to this issue, and it cannot be ruled out that in some jurisdictions third persons will be included in the scope of protection of the provision and in others not, until the issue is conclusively resolved by the European Court via a request by a national court for a preliminary ruling.

3.6 Presumption of Fault

Article 82(3), in turn, repeats that '[a] controller or processor shall be exempt from liability […] if it proves that it is not in any way responsible for the event giving rise to the damage'. Although that provision contains obvious similarities to the one in Article 23(2) of the repealed Data Protection Directive, it also has certain significant differences. It is the same in the sense that it again establishes a presumption of fault against the controller. But it also differs in two distinct ways: first, Article 82(3) clarifies that the presumption of fault burdens not only the controller, but also the processor. It will be interesting to see how this will apply in practice—it is possible that plaintiffs will address their claims against the data controller and the latter will have to exculpate himself by indicating the processor's liability. It is also possible that a plaintiff will address her claim against both, if she knows of the processor's existence.

Secondly, we can see in Article 82(3) another interesting modification in the wording: here the controller (or processor) may exculpate themselves only if they prove

that they are '**in no way responsible**' for the event giving rise to the damage. Article 23(2) of the repealed Data Protection Directive provided instead that the controller 'may be exempted from this liability, in **whole or in part,** if he proves that he is not responsible for the event giving rise to the damage' (emphasis added). If read correctly, the previous version of the exculpatory requirement stipulated that a court could allocate only part of the liability to the controller: to the extent that he was only partially responsible for the damage, he was obliged to compensate the plaintiff only partially as well. The new wording in the GDPR now excludes such possibility. In view of the joint-liability rule introduced in paragraphs 4 and 5 of Article 82 of the GDPR, the wording in Article 23 (2) of the repealed Data Protection Directive was irreconcilable and had to be amended. Hence, once the GDPR is applicable, if one of the persons responsible for even part of the harm is sued for damages, that person must indeed pay the whole compensation. He can then file for recourse against the other persons who are also (partly) responsible. The provision, however, should not be considered as restricting the defendant's right to claim and prove that the plaintiff was himself partly liable for the damage and to exculpate himself/herself accordingly.

3.7 Burden of Proof Regarding Infringement of the GDPR

Article 5(2) of the GDPR states that the controller shall be responsible for, and be able to demonstrate compliance with, the principles of lawful, fair and transparent data processing. This provision raises the question whether, under Article 82 of the GDPR, the defendant-controller has, in liability claims against him, the burden to prove that he was compliant with the GDPR rules and that he has not committed a data breach. If this interpretation is correct, the GDPR introduces a shift in the burden of proof to the benefit of the claimant filing for damages. According to another reading, however, the accountability requirement, provided for in Article 5(2) of the GDPR, exists only vis á vis the supervisory authorities and not vis á vis the claimant for the alleviation of his burden to prove the data breach. The correct interpretation of Article 82 in conjunction with Article 5(2) is, therefore, of paramount importance for the parties to a dispute and will undoubtedly soon become subject for review before the EU courts. Notably, in case the latter interpretation prevails and in view of the abolishment of some of the bureaucratic procedures of the Data Protection Directive, the burden of proof of the data breach may indeed have, in some instances, increased to the detriment of the plaintiff. The controller will, namely, often, have, under the GDPR, fewer obligations to evidence procedurally the proper execution of his data processing (since the controller does not, henceforth, need to follow an application process before a supervising authority and e.g. when no DPO or an impact assessment is required). Therefore, a procedural omission on the part of the controller shall not, it itself, constitute an easy to prove data breach and, so, in some cases, the proper execution of data processing could be taken for granted, unless

(successfully) challenged by data subjects or the supervisory authorities.[91] This may, indeed, at times signify an improvement of the defendant's position and the aggravation of the position of the plaintiff with regard to the proof of the GDPR infringement. On the other hand, the more rigid requirements of consent, provided for in the GDPR, may, to some extent, balance out such effect.

3.8 Statute of Limitations and Other Procedural Rules

The last paragraph of Article 82 of the GDPR provides guidance on the rules applicable for the exercise of the right to receive compensation: paragraph 6 clarifies that '[c]ourt proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2)'.[92] This provision, if further supplemented by an 'applicable law' clause, would have been extremely helpful with regard to a number of issues currently not answered by the Data Protection Directive and the GDPR—most indicatively, a limitation period (prescription) or the possibility of class actions. Where Member States have, for example, not included rules about prescription in the national data-protection acts with which they transposed the Data Protection Directive, there may be uncertainty about the application of such a prescription. In this respect, paragraph 6 of Article 82 may be in need of supplementing, which could take place in the national legislation for the complete implementation of the GDPR.

Finally, the GPDR expands the scope of the persons who may take initiative for the private enforcement of the data-protection rules: Article 80 gives the data subject 'the right to mandate a not-for-profit body, organization or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data […] **to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law**' (emphasis added). In view of the fact that many times data protection breaches give rise to a limited amount of damage to a large number of people, who may not have the resources and incentive to sue, this provision may indeed increase the frequency of data-protection actions, especially in jurisdictions with active consumer, human-rights and/or data-subject-rights protection institutions.

---

[91] See De Hert / Papakonstantinou (2012), 142.

[92] 'Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.'

3.9 Other Effects of the GDPR

3.9.1 Effects on the Requests for a Court Ruling

Article 79(1) of the GDPR reiterates the right to an effective judicial remedy against a controller and now includes the processor.[93] The reference here limits this right to the data subject: the choice is—to an extent—justified by the fact hat the judicial remedies envisaged mostly refer to rights of the data subject.[94]

In any case, the GDPR extends the current protection level of the data subject, who will henceforth be able to request a court order (an injunction relief) with regard, e.g. to his right to be informed,[95] the right of access to one's information,[96] the right to rectification,[97] the right to erasure,[98] etc.

The GDPR also expands the possibility of representation of the data subjects.[99] Article 80(1), namely, stipulates:

> The data subject shall have the right to mandate a not-for-profit body, organization or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf.[100]

Given that often data subjects refrain from enforcing their rights because of the legal costs involved in the process, this provision is very welcome.

---

[93] Compare Article 22 of the Data Protection Directive with the title 'Remedies': 'Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.'

[94] The provision does not apply directly to the right of Article 82 for compensation, as is evident from the fact that Article 82(6) expressly refers to Article 79(2) for its application also with regard to Article 82 GDPR.

[95] See Article 12 et seq. of the GDPR.

[96] See Article 15 of the GDPR.

[97] See Article 16 of the GDPR.

[98] See Article 17 of the GDPR (the so-called right to be forgotten).

[99] Such right was included in the Data Protection Directive only with regard to the supervisory authorities, see Article 28 para. 4: 'Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim'.

[100] Interestingly, Article 80(2) goes on to introduce the possibility for Member States to 'provide that any body, organization or association referred to in paragraph 1 of this Article, **independently of a data subject's mandate**, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing' (emphasis added).

Lastly, and as already mentioned above, the Regulation includes a provision on court jurisdiction: according to Article 79(2) proceedings against a controller or a processor may be brought before the courts of the Member State where the controller or processor has an establishment, or the courts where the data subject has her habitual residence (unless the former is a public authority acting in the exercise of its public powers).[101]

3.9.2 Effects on Other National Civil Claims

The new GDPR does not directly affect the other national civil provisions, either contractual or non-contractual. Nevertheless, it might have an indirect effect on them with regard to the following matters: first, the jurisdictional provision of Article 82(6) and its reference to Article 79(2) have an effect on the court competent for the claim raised on the basis of the same Article's liability clause; this could affect court jurisdiction also on other concurrent (raised with the same claim/brief) national civil claims. Second, the changes in the obligations of the controllers, (which, on the one hand, have become less procedural and bureaucratic but on the other hand, have rendered the controller accountable for the lawful, fair and transparent processing of the data towards the supervising authorities) introduce a shift on the manner with which the breach is now established. The prevailing interpretation of Article 5(2) in conjunction with Article 82, would, indirectly, affect the plaintiff's and defendant's burden of proof for the data breach, also in national civil claims. Third, the introduction by the GDPR of extended rights of the data subjects, should also affect the data breaches (and/or injunctions) that a claimant may invoke, also with regard to the civil claims based on the general national contract and tort provisions applicable in such cases. Finally, since the new liability regime of Article 82 of the GDPR seems more comprehensive and coherent, it could increase in importance with respect to the national civil provisions. The possibility for expanded representation of the data subjects in Article 82 claims by organizations (as prescribed in Article 80(1)) may also play a role in this effect, especially in jurisdictions where such organizations are active and/or rules on other collective-redress mechanisms rather weak.

4 Conclusions

The new GDPR has in some ways enhanced the protection of personal data: data subjects have extended rights and plaintiffs suffering harm for a data breach may file for restitution for their damage on the basis of the more comprehensive and coherent liability provision of Article 82. Many of the amendments and clarifications of this

[101] See Article 79(2) of the GDPR.

new provision are coming to (a) address the significant divergence in the liability rules transposing Article 23 of the repealed Data Protection Directive into national legislation and (b) complement such rules. These amendments are, therefore, mostly, very welcome; they include an explicit provision for compensation of moral damage, liability of the processor under certain conditions and joint liability of the persons who have jointly caused the damage, right of representation of the data subject by a competent association, etc. The new liability clause of Article 82 of the GDPR is, hence, expected to have a positive effect on the private enforcement of the data-protection rules; the harmonization effect of Article 82 GDPR, although not complete, is more than welcome as well.

References

Christodoulou, K. (2013), Data Protection Law (Dikaio Prosopikon Dedomenon), 2013 Nomiki Vivliothiki

Clifford, D. / Van Der Sype, Y.S. (2016), Online dispute resolution: Settling data protection disputes in a digital world of customers, 32 Computer Law & Security Review 272, Elsevier

De Hert, P. / Papakonstantinou, V. (2012), The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals, 28 Computer Law and Security Review 130, Elsevier

Van Dijk, N. / Gellert, R. / Rommetveit, K. (2016), A risk to a right? Beyond data protection risk assessments, Computer Law & Security Review 32 (2016), 286, Elsevier

Eickelpasch, J. (2016), Die neue Datenschutzgrundverordnung, 9/2016 Kommunikation & Recht 21, Fachmedien Recht und Wirtschaft

Foresman, A.R. (2015), Once More Unto the [Corporate Data] Breach, Dear Friends, 41:1 The Journal of Corporation Law 343, The University of Iowa

Franzen, M. (2016), BDSG § 7 Schadensersatz, in: T. Dieterich / P. Hanau / G. Schaub / R. Müller-GlÖge / U. Preis / I. Schmidt (Eds.), Erfurter Kommentar zum Arbeitsrecht, 16. Auflage 2016, C.H. Beck (cited: ErfK/author)

Gola, P. / Klug, C. / Körffer, Barbara (2015), BDSG § 7, in: P. Gola / R. Schomerus (Eds.), Bundesdatenschutzgesetz, 12. Aufl. 2015, C.H. Beck

Kanellopoulou-Mboti, M. (2016), Data protection breach sanctions (Kiroseis apo tin prosboli prosopikon dedomenon), in: Kotsalis, L. (Ed.), Personal Data (Prosopika Dedomena), 403-419, Nomiki Bibliothiki 2016

Korff, D. (2002), EC Study on Implementation of Data Protection Directive – Comparative Study of national laws, Human Rights Centre, University of Essex, available at: http://194.242.234.211/documents/10160/10704/Stato+di+attuazione+della+Direttiva+95-46-CE Kranenborg, H. (2015), Google and the Rights to Be Forgotten, 1 European Data Protection Law Review, 70

Kühling, J. / Martini, M. (2016), Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht? Europäische Zeitschrift für Wirtschaftsrecht 2016, 448

LRDP Kantor Ltd, Centre for Public Reform (2010), Comparative Study on different approaches to new privacy challenges in particular in the light of technological development, Final Report (20 January 2010), available at: http://ec.europa.eu/justice/data-protection/document/studies/files/new_privacy_challenges/final_report_en.pdf

Mitrou, L. (2010), Comparative Study on Different approaches to new privacy challenges, in particular in the light of technological developments, Country Studies, A.5. Greece, Final edit – May 2010, 3 et seq., available at: http://ec.europa.eu/justice/data-protection/document/studies/files/new_privacy_challenges/final_report_country_report_a5_greece.pdf

Palmer, G. (2015), UK - Google v Vidal-Hall (2015), A green light for compensation claims?, available at: http://www.linklaters.com/Insights/Publication1403Newsletter/TMT-News-June-2015/Pages/UK-Google-Vidal-Hall-green-light-compensation-claims.aspx
Piltz, C. (2016), Die Datenschutz-Grundverordnung, 9/2016 Kommunikation & Recht 557, Fachmedien Recht und Wirtschaft
Poullet, Y. (2006), The Directive 95/46/EC: Ten years after, 22 Computer Law & Security Report 206, Elsevier
Quass, S. (2013), BDSG § 7, in: H.A. Wolff / S. Brink (Eds.), Kommentar Datenschutzrecht, 11. Edition, 2013, C.H. Beck (Beck Online) (cited: BeckOK DatenSR/Quass)
Robinson, N. / Graux, H. / Botterman, M. / Valeri, L. (2009), Review of the European Data Protection Directive, (2009), Technical Report, available at: http://www.rand.org/content/dam/rand/pubs/technical_reports/2009/RAND_TR710.pdf
Robinson, G. (2012), Data protection reform, passenger name record and telecommunications data retention: Mass Surveillance Measures in the E.U, and the Need for a Comprehensive Legal Framework, 95 Critical Quarterly for Legislation and Law 394, Nomos Verlagsgesellschaft mbH
Sartor, G. (2013), Provider's liabilities in the new EU Data Protection Regulation: A threat to Internet freedoms?, 3 International Data Privacy Law, 3, Oxford Journals
Scheja, G. / Haag, N.C. (2013), Teil 5, in: A. Leupold / S. Glossner (Eds.), Münchner Anwaltshandbuch IT-Recht, 3. Aufl. 2013, C. H. Beck
Stylianou, K. / Venturini, J. / Zingales, N. (2015), Protecting user privacy in the Cloud: analysis of terms of service, 6 European Journal of Law and Technology, 1, available at: http://ejlt.org/article/view/462/593
Svantesson, D. / Clarke, R. (2010), Privacy and consumer risks in cloud computing, 26 Computer Law & Security Review, 391, Elsevier
Tremml, B. / Karger, M. / Luber, M. (2013), Der Amtshaftungsprozess, 4. Aufl. 2013, Vahlen
Van Alsenoy, B. (2012), Allocating responsibility among controllers, processors, and 'everything in between': the definition of actors and roles in Directive 95/46/EC, 28 Computer Law & Security Review 25, Elsevier
Voss, W.G. (2014/2015), European Union Data Privacy Law Developments (December 2014), Business Lawyer, Vol. 70, No. 1, 2014/2015, American Bar Association, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2572948
Wächter, M. (2014), Datenschutz im Unternehmen, 4. Aufl. 2014, C.H. Beck
Wright, D. / De Hert, P. (2012), Privacy impact assessment, media 2012, Dordrecht - Springer Netherlands

Additional Sources

Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor"', WP169, 16 February 2010, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf
Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor"', WP169, 16 February 2010, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf
Article 29 Working Party (2011), Letter from the Article 29 Working Party addressed to Vice-President Reding regarding the Article 29 WP's reaction to the Commission Communication "A comprehensive approach to personal data protection in the EU", 14.01. January 2011, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/2011_01_14_letter_artwp_vp_reding_commission_communication_approach_dp_en.pdf

Council of the EU, Council conclusions on the Communication from the Commission to the European Parliament and the Council – A comprehensive approach on personal data protection in the European Union, 3071st Justice and Home Affairs Council meeting Brussels, 24 and 25 February 2011, available at: http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/119461.pdf

Council of the EU, Information on the webpage of the Council of the EU, on the webpage of the Council of the EU, available at: http://www.consilium.europa.eu/en/policies/data-protection-reform/

European Commission, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union, COM(2010) 609 final, 4.11.2010, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52012DC0009&from=en

European Commission, Fact Sheet of January 2016, available at: http://ec.europa.eu/justice/data-protection/document/factsheets_2016/data-protection-factsheet_01a_en.pdf

European Commission, Joint Statement on the final adoption of the new EU rules for personal data protection, Brussels, 14 April 2016, available at: http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm

European Commission, Report from the Commission - First report on the implementation of the Data Protection Directive COM/2003/0265 final, available at: http://eur-lex.europa.eu/%20LexUriServ/LexUriServ.do?uri=CELEX:52003DC0265:EN:HTML

European Commission's site on the Status of implementation of Directive 95/46, available at: http://ec.europa.eu/justice/data-protection/law/status-implementation/index_en.htm

European Data Protection Supervisor (2011), Opinion of 14 January 2011 on the Communication from the Commission on "A comprehensive approach on personal data protection in the European Union", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf

European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Working Document (1 and 2) on a comprehensive approach on personal data protection in the European Union, 15.03.2011, available at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dt/859/859047/859047en.pdf

European Union Agency for Fundamental Rights (2013), Access to data protection remedies in EU Member States, available at: http://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies_en.pdf

Franet Contractor (2012), Ad Hoc Information Report, Data Protection: Redress mechanism and their use, United Kingdom, (2012), University of Nottingham Human Rights Law Centre, available at: https://fra.europa.eu/sites/default/files/access_to_data_protection_remedies_country_uk.pdf

Proposal for a Regulation COM(2012) 11 final of 25.1.2012, SEC(2012) 72 final, SEC(2012) 73 final, Explanatory Memorandum, p. 1, available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

UK Data Protection Authority, Information Commissioner's Office, available at <: https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/compensation/

Protecting Children Online: Combining the Rationale and Rules of Personal Data Protection Law and Consumer Protection Law

Milda Mačėnaitė

Contents

1 Introduction 332
2 Children as Data Subjects and Consumers Online: Defining Roles and Responsibilities 335
2.1 Consumers of 'Free' Services? 338
2.2 Legally (In)capable Consumers in (In)valid Consumer Contracts? 341
2.3 (In)competent Data Subjects? 342
3 Beyond the Obvious and Explicit: A Multitude of Raisons D'Être for a Specific Personal Data Protection Regime 343
3.1 GDPR and the Lack-of-Knowledge Yardstick 343
3.2 Different Online Behaviour, Needs and Privacy Perceptions 344
3.3 Particular Vulnerabilities and Immaturities 346
3.4 Learning from Consumer Law: Vulnerability as a Legislative Benchmark 347
3.5 Critical Understanding and Susceptibility 350
4 Combining the Safeguards of the Personal Data and Consumer Protection Regimes… Benefiting Children? 352
4.1 Child-Adapted Transparency 354
4.2 Fairness 360
4.3 Services Offered Directly to Children 364
4.4 Defining an Average Child 366
5 Conclusions 367
References 368

Abstract The newly adopted EU General Data Protection Regulation 2016/679 (GDPR) has explicitly recognised that children deserve more protection than adults, especially online. Yet, as the GDPR's child-specific protection regime is new and without precedent in Europe, both its underlying logic and its practical implementation

---

Milda Mačėnaitė received her PhD from Tilburg Institute for Law, Technology and Society (TILT).

M. Mačėnaitė (✉)
Tilburg Institute for Law, Technology and Society (TILT), Tilburg University, Tilburg, The Netherlands
e-mail: m.macenaite@uvt.nl

M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law*, MPI Studies on Intellectual Property and Competition Law 28, https://doi.org/10.1007/978-3-662-57646-5_13

remain unclear. The chapter explores the extent to which EU consumer law, which has already taken account of children as a particularly vulnerable group of consumers, can inform the newly adopted General Data Protection Regulation. The analysis focuses on the reasons justifying the child-specific protection regime, principles (fairness, transparency) in relation to children and conceptual questions (definition of an average child and services directed to children).

1 Introduction

Children and young people are often at the forefront of grasping the new and exciting opportunities that the Internet can offer, such as playing, communicating, experimenting with relationships and identities, learning, creating and expressing themselves. It is estimated that globally one in three Internet users are under the age of 18.[1] In being both early adopters and active users of the Internet, children are also becoming increasingly influential as consumers, especially in the digital-content market.[2] A growing preference for online shopping rather than for brick-and-mortar stores can be observed in Europe, despite the lack of reliable and recent EU-wide data about children's expenditure on digital goods and services.[3] Young people using the Internet in particular show a big increase in online purchasing. In 2016, almost 70% of Internet users aged 16–24 in Europe had bought goods or services online.[4]

Although the level of children's perception and attitudes towards online shopping varies and is influenced by many factors, such as age, parental guidance, social networks and peers,[5] and smaller children still might prefer physical over digital stores due to the variety of goods and instant gratification,[6] children undoubtedly as a consumer market have become very attractive for sellers and marketers. In fact, children are known to be a three-layer market: a primary market for their own purchasing power related to pocket money or income, an influence market, as children influence the buying patterns of their parents, and a future market, given their future spending power as purchasing habits and preference for brands continue into adulthood.[7]

Yet children are increasingly acting not only as consumers but also and at the same time as data subjects in their online activities. In the current data-driven

[1] Livingstone / Carr / Byrne (2015).

[2] Helberger / Guibault / Loos / Mak / Pessers / Van der Sloot (2013).

[3] The numbers of children purchasing, for example, apps online are significant. According to the European Commission (which cites an external study of Bitkom) only in Germany from 2012 to 2013 in-app purchases doubled amounting to 240 million EUR. More than one million of the app users were individuals aged between 10 and 19 years. European Commission (2014b).

[4] Eurostat (2016).

[5] Thaichon (2017).

[6] Boulay / de Faultrier / Feenstra / Muzellec (2014).

[7] Buckingham (2000).

information economy and the proliferation of the Internet of Things, almost any 'smart' service or product comes with the collection of personal data and it is hard to imagine anyone being a consumer[8] without becoming a data subject (a natural person whose personal data is processed). As noted by Helberger et al., '(w)ith the integration of more and more data into consumer products, many data protection issues also become consumer issues, and vice versa'.[9] Consequently, there is a growing tendency to speak of consumers' rather than individuals' rights to data protection[10] and to look for an integrated vision of 'data consumer law',[11] reinforcing the close relationship between the roles of data subjects and consumers in the digital environment.

As '(p)ersonal data are economic assets, and are used to develop modern services, to categorise consumers, and to influence consumers',[12] the roles of consumers and data subjects are intertwined and the switch from the former to the latter can be hardly noticeable from a practical perspective. On a daily basis, consumers conclude agreements and consent to the collection of their data without necessarily fully realising that by simply ticking 'I agree' buttons on a website or adjusting device settings they consent to their data collection and use. For example, in order to create an account on social-networking sites, users accept the terms of use (virtually sign a legally binding contract as consumers) and consent to their personal data being processed by agreeing to the privacy policy of a site (act as data subjects).[13]

Widely spread business practices, such as combining contracts with consent (consent bundling),[14] when consumers allow collection and analysis of their personal data in addition to the provision of the main 'agreed' service, further contribute to blurring the line between consumers and data subjects and increase 'datafication',[15] which results in constant and opaque collection of consumers' personal data. In fact, the datafication of children's online activities is an increasingly growing research area, with studies examining digital dataveillance practices and their potential impact on children and their rights[16] and critically analyzing advertising, branding and marketing in games and apps directed towards children.[17]

[8] Consumer is defined as 'any natural person who is acting for purposes which are outside his trade, business or profession' Article 2(b), Directive 93/13/EC.

[9] Helberger / Borgesius / Reyna (2017), 1428.

[10] Leczykiewicz / Weatherill (2016).

[11] Helberger / Borgesius / Reyna (2017), 1429.

[12] Helberger / Borgesius / Reyna (2017), 1430.

[13] Wauters / Lievens / Valcke (2015).

[14] Article 7(4) and Recital 43 of the General Data Protection Regulation (2016/679) create a presumption that consent bundling will render consent invalid as not 'freely given'.

[15] Mayer-Schönberger / Cukier (2013).

[16] Lupton / Williamson (2017).

[17] Grimes (2015).

Although the EU has paid specific attention to the vulnerability of children as consumers in the Directive 2005/29/EC on Unfair Commercial Practices,[18] protection of children's informational privacy has been designed to conflate adults and children in one single group of data subjects. Since 1995, minors have been covered by the age-neutral data protection provisions of Directive 95/46/EC with no special focus on the processing of children's data, despite the fact that on a normative level, it is clearly acknowledged that a child's right to privacy needs to be considered separately from an adult's right to privacy.[19]

The newly adopted EU General Data Protection Regulation (2016/679)[20] (GDPR) has significantly changed the status quo and rejected the 'age-blind' approach to data subjects. For the first time, it explicitly recognises that children need more protection than adults, especially online, as 'they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data' (Recital 38). Such specific protection is afforded through a new two-tiered child-specific protection regime.[21] As the GDPR child-specific protection regime is new and without precedents in Europe,[22] both the underlying logic and the practical implementation of it remain unclear. For example, a lack of clarity exists about conceptual questions (definition of an average child and services directed to children) and principles (fairness, transparency) in relation to children.

The aim of this chapter is to explore the extent to which EU consumer law, which has taken account of children as a particularly vulnerable group of consumers, can inform the GDPR and reduce the clarity gap in relation to the above-mentioned GDPR concepts and principles.

---

[18] Directive 2005/29/EC of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (Unfair Commercial Practices Directive), 11 June 2005, L149/22.

[19] For example, Livingstone / Carr / Byrne (2015), 15 claim that '*greater steps are needed, because children's human rights necessitate special provision (special protection measures, best interest of the child, evolving capacity, participation, and so on), and there are good reasons to be concerned about whether children's rights will be met even where children and adults' rights are the same. This is because infringements of harm generally have a disproportionate impact on the vulnerable, and thus an approach that is age-generic (arguably, age-blind, by analogy gender-blind or disability-blind approaches) is unlikely to suffice*.'

[20] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4 May 2016, 1–88.

[21] For a more detailed description of the two-tiered child-specific protection GDPR regime see Mačėnaitė (2017).

[22] This regulatory effort is new for the EU, but the US almost two decades ago adopted detailed rules for the operators that collect personal information from children under the Children's Online Privacy Protection Act (COPPA). See Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505. For a detailed comparison between the requirements stipulated in the COPPA and the new rules in the EU see Mačėnaitė / Kosta (2017).

The chapter is structured as follows. First, it defines consumers and data subjects in today's data-driven online environment and explores the legal qualification of the two roles in the case of children. It then examines the justifications for having a specific child-tailored data protection regime, going beyond the GDPR's obvious and explicit lack-of-knowledge yardstick. It broadens the view and takes into account the insights from social sciences on particular vulnerabilities and needs of children, as well as from consumer law and its legal vulnerability benchmark, partially embodying the social science insights. Finally, the chapter explores how consumer protection can inform data protection law by: (1) improving transparency through the information on data collection adapted to the specific needs and age of children; (2) enhancing fairness of data processing; (3) delineating services offered directly to children (4) defining an average child to decide when a child is able to provide a valid consent for the processing of his or her personal data.

2 Children as Data Subjects and Consumers Online: Defining Roles and Responsibilities

In the majority of the consumer law legal instruments 'consumer' is defined as a natural person who enters into a contract which falls outside his trade or profession.[23] This definition might prove problematic for adults. If interpreted in a narrow sense, it could encompass individuals who use online services for both personal and professional purposes, for example to send professional emails from their personal email accounts, to store work-related documents on cloud storage services etc. This definition is less problematic for minors, who are rarely engaged in professional activities or trade.

However, a more relevant distinction for children is that between consumers and prosumers and between data subjects and data controllers. Children, in particular adolescents, actively take part in the collaborative or sharing economy and become co-creators of digital products and services. For example, children not only consume video games but also produce artefacts in the game-related affinity spaces,[24] not only watch but also create and monetise digital content, such as videos, through advertising run on them on YouTube or blog posts through product endorsement and promotion. As technological developments and advancements, such as open design, additive manufacturing, crowd sourcing and open data, allow users to be a producer and a consumer at the same time, 'prosumer' as a legal concept escapes a clear legal definition, resulting in legal uncertainty about relevant rights and responsibilities. For example, when a third party (e.g. crowdsourcing platform) sells the co-created product and prosumers get part of the profit, an individual can be considered in a trade or business relation with the platform (i.e. producer) and might

[23] Article 2(b) of Unfair Contract Terms Directive, Article 2(a) of Unfair Commercial Practice Directive, Article 2(1) of Consumer Rights Directive.

[24] Wu (2016).

not be necessarily protected by consumer law in all cases.[25] Due to the unclear legal distinction between consumers, producers and prosumers, facts play a key role in courts when deciding if an individual qualifies as a consumer and 'the turnover, the amount of products, frequency or time involved in an activity of a prosumer helps to define in which quality a person acts'.[26] Also, due to the fact that consumers co-create their products or services, lack of clarity exists in relation to insurance coverage of potential accidents or the qualification of consumers when producing the goods and services.[27]

A similar shift is reflected in scenarios when Internet users change roles from data subjects to data controllers, losing the rights granted by data protection law. In line with its predecessor, the GDPR includes the 'household exception' (Article 2(c) GDPR). It clearly states that the Regulation 'does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity', such as social networking and online activity undertaken within the context of personal correspondence (Recital 18). However, the exact meaning of 'personal or household activity' is not entirely clear. The Court of Justice of the European Union (CJEU) in the *Lindqvist* case[28] concluded that the household exception is not applicable when information is accessible 'to an indefinite number of people', but the exact meaning of 'an indefinite number of people' lacks clarity. In the same vein, the Article 29 Working Party has acknowledged that a user 'may acquire a high number of third party contacts, some of whom he may not actually know' and this 'could be an indication that the household exception does not apply'.[29] As a result, the user who acts online and discloses personal data to a high or indefinite number of people could be considered a data controller and be obliged to comply with all the obligations stemming from the GDPR.

Such a provision no longer reflects the reality of today's data-driven online environment and expanded data processing capabilities of amateurs, and might have unintended consequences for social-network users.[30] Scholars have argued that it would be too burdensome to apply data protection rules to private individuals[31] and that supervisory authorities could not ensure compliance[32] and have noted even possible interference with individuals' fundamental right to privacy.[33]

---

[25] Weitzenböck (2014).

[26] Valant (2015), 16.

[27] Valant (2015), 16.

[28] ECJ, Criminal proceedings against Bodil Lindqvist, C-101/01, ECLI:EU:C:2003:596, para. 46-58.

[29] Article 29 Data Protection Working Party, Opinion 5/2009 on Online Social Networking, WP 163, 2009, 6.

[30] Helberger / Van Hoboken (2010); Xanthoulis (2014).

[31] Garrie / Duffy-Lewis / Wong / Gillespie (2010).

[32] Wong / Savirimuthu (2008); Xanthoulis (2014).

[33] Article 29 Data Protection Working Party (2013), Statement of the Working Party on current discussions regarding the data protection reform package - Annex 2 Proposals for Amendments regarding exemption for personal or household activities.

On the other hand, excluded from the scope of data protection law harmed individuals would lose the possibility to lodge a complaint as data subjects and would need to opt for more burdensome civil-law actions (defamation, the right to protection of one's image) in courts.[34] Some potential solutions proposed, yet not directly implemented in the GDPR, include using a combination of five criteria to decide whether the household exemption applies to a particular processing activity: publicity of the disclosed data, types of data subject involved, scale and frequency of the processing, whether the activity is carried out singly or as a collective, and adverse impact.[35] Data protection authorities referring to these criteria would become more objective and gain a certain degree of discretion when deciding whether to take action in a specific situation.

When considering online behaviour, the application of data protection rules to children as data controllers appears to be theoretically probable even if undesirable. Empirical evidence suggests that adolescents have more contacts on social networks than adults or young adults and add more unknown people to contact lists simply as they want to know them or because they are popular or famous.[36] Networks of 'friends' tend to grow during the upper secondary school years and generally amount to approximately 500 contacts.[37] Given the conventional understanding of the data protection framework, it is unlikely that finding children to be data controllers could be clearly excluded. However, as discussed below, the positioning of children as competent data subjects is already challenging and debatable and thus, the assignment of the complex duties and obligations imposed on data controllers may be even more problematic.

Nevertheless, from a theoretical perspective it is interesting to explore how data protection law could accommodate children as data controllers even if the household exemption did not apply. More specifically one could question whether a child could benefit from the exemption for the purposes of artistic or literary expression in the context of using a social network and thus how the balance between freedom of expression and the right to privacy could be struck in such circumstances. In addition, one could question how legitimate interests as a condition for lawful processing in Article 6(1)(f) of the GDPR would be interpreted if a child is deemed to be a data controller and also how the 'legitimate grounds' for refusing the exercising of data subject rights could operate in practice. These abstract questions may have practical consequences and therefore may only be made clear via case law and CJEU interpretation. In the interim, however, doubt and room for abstract legal reasoning remain. As such, more research is required in this area.

---

[34] Article 29 Data Protection Working Party (2013), Statement of the Working Party on current discussions regarding the data protection reform package - Annex 2 Proposals for Amendments regarding exemption for personal or household activities.

[35] Article 29 Data Protection Working Party (2013), Statement of the Working Party on current discussions regarding the data protection reform package - Annex 2 Proposals for Amendments regarding exemption for personal or household activities.

[36] Steijn (2014).

[37] Mantelero (2016).

2.1 Consumers of 'Free' Services?

Consumer protection has typically dealt with markets where products and services are traded in exchange of money. In fact, consumer rights have been traditionally guaranteed in sales and service contracts when the consumer pays a 'price', meaning payment in money, vouchers, gift cards or loyalty points with a specified monetary value rather than the services promoted by the trader as 'free'.[38] However, in the current data-driven information society the distinction between paid and 'free' electronic services has become obsolete both in theory and in practice. Paying not only with money but also with (personal) data for digital services and content has become an increasingly important way of bargaining online.

Such bargaining is particularly popular among younger Internet users, as various studies in Europe[39] and North America[40] report that the most favourite websites among children are those that do not require their users to pay for their services in terms of money, such as YouTube, Facebook and Google.

Although hidden costs of free services[41] and their detriment to consumers[42] have long been acknowledged by academics, the regulation of contracts in which a consumer 'pays' for a product or service by providing personal or other data to the supplier has been much slower.[43] Nevertheless, in its recent draft of a Directive on certain aspects concerning contracts for the supply of digital content (the proposed Digital Content Directive),[44] aiming to regulate digital content contracts such as downloading or web streaming of movies or digital services like cloud storage or social media, the European Commission has broadened the understanding of regular contract law, explicitly putting contracts in which the counter-performance refers

[38] European Commission, DG JUSTICE Guidance Document concerning Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, 13 June 2014 (hereinafter - Guidance Document concerning Directive 2011/83/EU).

[39] Livingstone / Haddon / Görzig / Ólafsson (2011).

[40] Steeves (2014b).

[41] Bradshaw / Millard / Walden (2011); Helberger / Guibault / Loos / Mak / Pessers / van der Sloot (2013); Loos / Luzak (2016).

[42] Hoofnagle / Whittington (2016).

[43] 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 (E-Commerce Directive) OJ L 178, 17 July 2000, 1–16, does not exclude information society services financed by advertising from its scope: *'information society services are not solely restricted to services giving rise to on-line contracting but also, in so far as they represent an economic activity, extend to services which are not remunerated by those who receive them, such as those offering on-line information or commercial communications, or those providing tools allowing for search, access and retrieval of data'* (Recital 18).

[44] Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, 2015/0287 (COD).

to the payment of a price on equal basis with contracts where 'the consumer actively provides counter-performance other than money in the form of personal data or any other data' (Article 3(1)). Until this explicit acknowledgment of personal data as actual online currency, there were only sporadic references to this issue in several consumer-related EU guidance documents. The European Commission's guidance document on unfair commercial practices refers to 'increasing awareness of the economic value of information related to consumers' preferences, personal data and other user-generated content'.[45] It stresses the importance of being transparent and informing consumers how their preferences, personal data and user-generated content are going to be used.[46] If consumers are not informed then the marketing of products that requires the exchange of personal data of users as 'free' could constitute a misleading practice.[47] Also, recently the Consumer Protection Cooperation Network in the social media context stressed that the Directive 93/13/EC on Unfair Contract Terms is applicable to all types of contracts between consumers and businesses, explicitly mentioning as an example 'contracts where consumer generated content and profiling represent the counter-performance alternative to money'.[48]

Similarly, although without an explicit reference to personal data, the Directive 2011/83/EU on Consumer Rights (Consumer Rights Directive)[49] does not fully exclude 'free' online services from its scope and legal requirements. It distinguishes between sales and service contracts and contracts for the supply of online digital content.[50] Contrary to the definition of sales and service contracts, the Directive does not mention 'payment' for the digital-content contracts. Therefore, according to the European Commission, 'the Directive would seem to apply also to contracts for the supply of (…) online digital content even if they do not involve payment', such as the contracts for a free download of a game from an app store.[51] However,

[45] European Commission, Commission Staff Working Document, Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices, 25 May 2016, SWD(2016) 163 final, 97.

[46] European Commission, Commission Staff Working Document, Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices, 25 May 2016, SWD(2016) 163 final, 97.

[47] European Commission, Commission Staff Working Document, Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices, 25 May 2016, SWD(2016) 163 final, 97.

[48] Consumer Protection Cooperation Network (2017), 3.

[49] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance, OJ L 304, 22 November 2011, 64–88.

[50] It is not entirely clear how certain online services should be qualified: for example, should social-networking sites (SNSs) be considered as services or digital content? When the user signs up for a SNS he agrees to the terms of use or terms of service – a legally binding contract of service provision. The proposed Digital Content Directive, however, considers SNSs as being governed by provision of digital content contracts.

[51] European Commission, Guidance Document concerning Directive 2011/83/EU, 8.

express contractual agreement needs to be concluded between consumers and traders and a mere access to a website is not necessarily considered a contract.[52] Therefore, 'contracts (for the supply of digital content in exchange of data) that are concluded by tacit agreement would escape the application of the Consumer Rights Directive'.[53]

That being said, it is unclear how this line of argumentation aligns with Article 5(3) of the ePrivacy Directive[54] which requires prior informed opt-in consent for storage and access to information on users' terminal equipment. It is uncertain how the collection of personal data via cookies for commercial purposes could be seen as a tacit agreement. In this regard, one could refer to the European Data Protection Supervisor's criticism of the proposed Digital Content Directive which delineates active and passive data collection despite the ePrivacy Directive's provisions.[55] Accordingly, there is a huge amount of debate and confusion surrounding a correct interpretation of the positioning of consent and its relationship with contract and contractual protections.

In the same vein, the GDPR seems to hint that its scope extends to unpaid online services, i.e. to the processing of personal data when offering goods or services to data subjects in the EU, irrespective of whether a payment is required of the data subject (Article 3). Yet in Article 8 defining the conditions applicable to child's consent in relation to information society services the GDPR also explicitly refers to paid services, as information-society services are defined as 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services' (Point b of Article 1(1) Directive 2015/1535[56]). At first glance therefore it may seem that the reference to electronic services provided for remuneration requires direct remuneration from the users. However, in practice the phrase 'normally provided for remuneration' has been assigned a broad meaning. The CJEU has explained the concept of remuneration in various cases. It has ruled that the important element is that the remuneration is given to the provider of the service but it is not necessarily the recipient who has to give the remuneration. In *Belgium v Humbel* the CJEU considered that 'the essential characteristic of remuneration (…) lies in the fact that it constitutes consideration for the service in question'.[57] In *Bond van Adverteerders v Netherlands*, the CJEU found that the remuneration could come from an external party, such as an advertiser, and not

[52] European Commission, Guidance Document concerning Directive 2011/83/EU, 64.

[53] Helberger / Borgesius / Reyna (2017), 1444.

[54] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive), OJ L 201, 31.07.2002, 37 – 47.

[55] EDPS (2017).

[56] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, OJ L 241, 17 September 2015, 1-16.

[57] ECJ, Belgium v Humbel, C-263/86, ECLI:EU:C:1988:451, para. 17.

necessarily from the recipient of the service.[58] The CJEU has explained the concept of remuneration in the context of services offered within the European Union. It is unclear, however, if a service should be deemed distinct from a service contract, given that contract law remains largely dominated by national contract law vis-à-vis the requirements for contract formation.[59]

2.2 *Legally (In)capable Consumers in (In)valid Consumer Contracts?*

There is no clear definition of 'child' in the EU consumer law. The Unfair Commercial Practices Directive includes some provisions designed to protect children against unfair commercial practices, but does not specify who is a child. The guidance document issued by the European Commission on this directive mentions not only children but also teenagers as vulnerable consumers, but equally fails to provide concrete age ranges.[60] An interesting exception is the Toy Safety Directive,[61] where the concept of 'child' is linked to the notion of 'toy'. The Directive is applicable to 'products designed or intended, whether or not exclusively, for use in play by children under 14 years of age (hereinafter referred to as toys)' (Article 2.1).

Regulation or self-regulation fills this gap in certain cases on a national level. For example, the UK Code of Non-broadcast Advertising, Sales Promotion and Direct Marketing, adopted by the UK's Advertising Standard Authority, defines a child as an individual under 16.[62] In addition, as a general principle it acknowledges that 'the way in which children perceive and react to marketing communications is influenced by their age, experience and the context in which the message is delivered' and therefore, these factors are considered when examining whether specific marketing communication complies with the code. Interestingly, the age threshold to become a data subject is much lower in the same code. Advertisers are allowed to collect personal data from children over 12 years old without parental consent.[63]

When defining a 'child' in consumer law, contract law is relevant to establish when a child may enter into contractual relations, but even contract law does not help in qualifying pre-contractual relations, such as product marketing or other commercial practices. In the majority of the national laws children are not considered legally capable to enter into valid contracts or do not have the competence to conclude agreements without parental permission. This prohibition follows from

[58] ECJ, Bond van Adverteerders v Netherlands State, C-352/85, ECLI:EU:C:1988:196, para. 16.

[59] See Clifford / Van Der Sype (2016), 279-280.

[60] European Commission, Commission Staff Working Document, Guidance on the Implementation /Application of Directive 2005/29/EC on Unfair Commercial Practices, 25 May 2016, SWD(2016) 163 final.

[61] Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys, OJ L 170, 30 June 2009, 1.

[62] UK Advertising Standard Authority (2010).

[63] UK Advertising Standard Authority (2010).

the assumption that minors are not fully capable of understanding the nature and legal consequences of their acts. Nevertheless, children between the ages of 14 and 18 in various jurisdictions are allowed to consent to agreements in small, day-to-day activities, such as those related to their income or daily life (e.g. buy food, clothes, transport tickets), without the involvement of their legal representatives.[64] For example, in Finland children under 15 can purchase only ordinary goods of small significance, such as spending their pocket money, without parental consent.[65]

The limits of the legal capacity to act online are much less clear. According to Wauters et al., actions of underage social-network users can have legal consequences if they can be qualified as 'daily acts' as well as if the minors are able to understand the scope of their actions (have reached the age of discernment).[66] A contract concluded by a minor who has not yet reached the age of discernment will be considered invalid or void.

The question of whether a minor can conclude a valid agreement online, e.g. accept the terms of service of a web-based service, should be answered according to the national contract law. For example, in Belgium a concluded standard contract is valid if the user has actual knowledge of the content of the contract and accepts the agreement.[67] Availability, visibility and comprehensibility of the contract terms are important, but the existence of actual knowledge has to be decided by a judge in a specific case.[68]

2.3 (In)competent Data Subjects?

Defining the 'legal competence' of children to consent to their personal data processing is a complicated task. Although the GDPR mandates the establishment of clear age thresholds (leaving it to the Member States to define the precise age between 13 and 16 years), diverging age thresholds have been already explicitly introduced (or tacitly accepted in practice, depending on the Member State) for minors as data subjects while regulating their power to give valid consent to the data processing operations.[69] In general, many European countries consider minors of 14, 15 or 16 years as competent to consent to the processing of their data.[70]

---

[64] For a comparative overview of the legal capacity of minors in contract law see Loos / Helberger / Guibault / Mak / Pessers / Cseres / van der Sloot / Tigner (2011), 138-141.

[65] Finnish Competition and Consumer Authority (2015).

[66] Wauters / Lievens / Valcke (2015).

[67] Wauters / Lievens / Valcke (2015).

[68] Wauters / Lievens / Valcke (2015).

[69] Mačėnaitė / Kosta (2017).

[70] Dowty / Korff (2009). It should be noted that given the upcoming implementation of Article 8 of the GDPR and the revision of national data protection laws that are under way, the age of consent thresholds are expected to change. Due to influence from the US, many EU Member States may choose to deviate from the current status quo of 14, 15 or 16 years old and lower the age threshold to 13 years.

Prior to the GDPR, a few national data protection laws in the EU have explicitly stated the exact age threshold from which minors are treated as legally competent to act as data subjects on their own behalf.[71] Other national legal frameworks did not include specific provisions, but relied on the legal capacity of minors as actors in civil law or assess the concrete situation on a case-by-case basis.[72] In the latter case, the general criteria of the best interest of the child, the level of moral and psychological development, the capacity to understand the consequences of giving consent and evaluating specific circumstances (the age of the child, the purpose of data processing, type of personal data involved, etc.) were taken into account in carrying out the assessment.[73] Such evaluation of the capacity of the data subject is a context-specific rather than universally applicable test, but assumption-based exemplary age thresholds were normally set in case law, legal doctrine or guidelines from the data protection authorities.[74]

3 Beyond the Obvious and Explicit: A Multitude of Raisons D'Être for a Specific Personal Data Protection Regime

The GDPR justifies its child-specific provisions exclusively in light of children's potentially lower awareness about the risks and safeguards related to the collection and use of their data. However, if the only reason for protecting children and young people was a lack of awareness, this problem could be addressed by intensive awareness-raising activities and would not necessarily require legislative action.[75] The following sections aim to explore the various additional factors which motivate the establishment of a specific, child-tailored data protection regime.

3.1 GDPR and the Lack-of-Knowledge Yardstick

The GDPR refers to children's lower awareness as a yardstick providing a normative justification for establishing its specific child-protection regime. Lack of knowledge and of a full understanding of complex personal data-collection practices,

[71] Prior to the GDPR, parental consent was required for the processing of personal data of children under the age of 14 in Spain (Article 13 of the Spanish Royal Decree 1720/2007 of 21 December) and 16 in the Netherlands (Article 5 of the Dutch Personal Data Protection Act (25 892) of 23 November 1999) and Hungary (Section 6 (3) of the Hungarian Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information).

[72] Mačėnaitė / Kosta (2017).

[73] Belgian Privacy Commission (2002); Article 29 Data Protection Working Party, Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools), WP 160; Dowty / Korff (2009).

[74] Mačėnaitė / Kosta (2017).

[75] It should be acknowledged that effective awareness raising that leads to long term behavioural changes is not an easy objective to achieve. See Jones / Mitchell / Walsh (2013) for the analysis of online child safety education in the US.

along with their implications, especially online, is an undeniable problem not only for children and young people, but for many adults too. Research shows that some more advanced data-collection and tracking techniques, such as canvas fingerprinting and evercookies and their possible impact, are hard to understand even for sophisticated users.[76] Websites that are popular among children employ increasingly sophisticated methods to gather children's data as they play, communicate or browse online, resulting in constant surveillance. As Montgomery points out, the goal of these surveillance practices, used on many websites, is to create a cognitive, emotional and behavioral relationship between the child and the website, through micro-targeted 'one-on-one' marketing and communication strategies.[77] Similar worries about the commercial surveillance of children in networked spaces, and the subsequent effects this may have, have been raised by a number of academics.[78]

For young people, privacy policies are long, complex, difficult to find and often age-inappropriate.[79] The privacy policies of the most widely used social-networking sites, such as Facebook and Twitter, can easily confuse users by valorising 'sharing' and 'control', despite the ongoing ubiquitous collection, use and disclosure of their data.[80]

Even though some children might be tech-savvy and informed Internet users, this does not necessarily render them capable of fully realising the consequences of pervasive online data-collection practices. For example, children do not intuitively perceive their online actions as actions that are being constantly monitored.[81] Even the mere positioning of children as 'digital natives'[82] or as part of 'the Net generation'[83] has been widely debated in academic literature.[84] Empirical evidence suggests that other factors such as breadth of use, experience and education are in some cases even more decisive than generational differences in defining someone as a 'digital native'.[85]

3.2 Different Online Behaviour, Needs and Privacy Perceptions

The GDPR refers only to the (lack of) certain capacities pertaining to children rather than to the specific features characterising children, and especially adolescents, as individuals. Developmental psychology provides evidence that adolescents have

[76] Acar / Eubank / Englehardt / Juarez / Narayanan / Diaz (2014).

[77] Montgomery (2015).

[78] Grimes (2015); Montgomery (2015); Rooney / Taylor (2017).

[79] Micheti / Burkell / Steeves (2010); Grimes (2013).

[80] Steeves (2017).

[81] Savirimuthu (2016).

[82] Prenksy (2001).

[83] Tapscott (1998).

[84] Jones / Shao (2011), Helsper / Eynon (2010).

[85] Helsper / Eynon (2010).

particular needs and interests, such as identity formation, developing their agency and establishing autonomy, and creating peer relations.[86]

Making friends and forming peer relations become increasingly important with growth and can even affect the psychological, social and academic development of adolescents.[87] Adolescents are eager to make new friends[88] and often establish more friendships than adults.[89] In contrast, young adults feel more of a need to make the existing relationships more intimate and satisfying.[90] Adults spend less time with friends than do adolescents.[91] These claims are confirmed in the social-media context by several authors in Europe and beyond. In the Netherlands, Steijn and Schouten showed that younger social media users tend to create new relationships more often, while older users often strengthen ties with existing friends.[92] In the same vein, Mantelero found that with increasing age adolescents in Italy consider it less important to look for new friends on social networks but rather communicate with existing friends or family members.[93] The same trend is confirmed by Third et al. in relation to children from 16 countries around the world.[94]

Identity creation is an equally important need during adolescence.[95] Adolescents spend a lot of time with their peers, who become important circles where adolescent's identity is established.[96] Boneva et al. state that '[a]dolescence is defined by the need for intense person-to-person communication with a friend—spending a lot of time together (…) and self-disclosing'.[97] Valkenburg and Peter show that the Internet has become a new arena for adolescents to present and experiment with their identities.[98] In contrast to children, older individuals have already developed their identities[99] and are willing to make them more solid and adults 'have less of a need to experiment with their identities or to present themselves favourably to others'.[100] Identity development and creation of relations as developmental needs

[86] Greenfield / Gross / Subrahmanyam / Suzuki / Tynes (2006); Subrahmanyam (2008); Subrahmanyam / Garcia / Harsono / Li / Lipana (2009).

[87] Blieszner / Roberto (2004); Savin-Williams / Berndt (1990).

[88] Boneva / Quinn / Kraut / Kiesler / Shklovski (2006).

[89] Hartup / Stevens (1999); Blieszner / Roberto (2004).

[90] Erikson (1968).

[91] Hartup / Stevens (1999); Blieszner / Roberto (2004).

[92] Steijn (2014), Steijn / Schouten (2013).

[93] Mantelero (2016).

[94] Third / Bellerose / Dawkins / Keltie / Pihl (2014).

[95] Erikson (1959).

[96] Brown (1990), 179.

[97] Boneva / Quinn / Kraut / Kiesler / Shklovski (2006), 618.

[98] Valkenburg / Peter (2008).

[99] Waterman (1982).

[100] Steijn (2014), 51.

are potentially connected with user online behaviour, such as adding contacts on their social networks and disclosure of personal information.[101]

Academics have established the link between developmental phases and online behaviour in relation to adolescents.[102] Empirical research also has elucidated that privacy perceptions and concerns are different between children, adolescents and adults. In particular, as claimed by Steijn, a developmental perspective can help to understand, and thus justify, the different privacy concerns and behaviour of individuals of different ages on social media.[103] Steijn relies on empirical evidence gathered in the Netherlands from 16,000 individuals in three age groups: adolescents (12- to 19-year-olds), young adults (20- to 30-year-olds) and adults (31-year-olds and older). He shows that behaviour of individuals on social media (e.g. having more contacts, posting information more frequently) can be related to characteristics that are typical for adolescents, young adults and adults in their life stages.[104] Thus, developmental characteristics of relationship development and identity development are related to user behaviour on social media and can partially explain the lower concerns for privacy among adolescents.

3.3 Particular Vulnerabilities and Immaturities

The reliance on neurotechnology, in particular magnetic resonance imaging, in the last decade has provided neurological evidence to compare the different structures and functioning of adolescent and adult brains. Scientists have demonstrated that there are structural and functional immaturities in the brain of adolescents.[105] This has resulted in the questioning of Jean Piaget's previously dominant claim that by the age of 15, adolescents' cognitive capability to understand, appreciate, and articulate decisions are on par with those of an adult.[106] It has been instead acknowledged that 'teenagers may have the *ability* to reason like adults, but do so with "vexing inconsistency"'[107] due to, among others, their emotional volatility, impulsiveness, lower ability to deflect the pressure of peers.

Since the part of the brain controlling inhibitions fully matures only in early adulthood, adolescents can be less capable of evaluating risky situations and can be more

[101] boyd (2008); Boneva / Quinn / Kraut / Kiesler / Shklovski (2006); Peter / Valkenburg (2011).

[102] Peter / Valkenburg (2011).

[103] Steijn (2014).

[104] Steijn (2014).

[105] Giedd (2008); McAnarney (2008); McCreanor / Barnes / Gregory / Kaiwai / Borell (2005); Steinberg (2007, 2008).

[106] Cited in Preston / Crowther (2014), 454-455.

[107] Preston / Crowther (2014), 451.

easily misled.[108] They are less likely to consider the long-term consequences of their actions, and are more likely to be risk-prone.[109] As summarised by Preston and Crowther, '(n)otwithstanding growing research on the capabilities of teenagers and their need for respect and autonomy, the developmental science shows that, alongside these positive qualities, minors are nonetheless still impulsive, take more risks than adults, and are less capable of controlling their emotions'.[110] The authors continue: '(t)hese behavioral immaturities suggest that minors are not in the same position as adults when making long-term decisions, especially when surrounded by their peers' and further note that 'in the Internet age, they are always surrounded by their peers, using social media to bounce every decision off a host of other teenagers'.[111]

These specific developmental features might influence their online behaviour and increase the possibility of online victimisation among peers, as well as the possibility of commercial personal data exploitation, to a level higher than that of cases involving younger children or adults. In the latter case, for example, online marketers can employ special strategies to take advantage of the adolescents' vulnerabilities, knowing that '[b]ecause of adolescents' emotional volatility and their tendency to act impulsively, they are also more vulnerable than adults to such techniques as real-time bidding, geolocation targeting (especially when an individual is near a point of purchase) and 'dynamic creative' adverts tailored to their individual profiles and behaviour patterns'.[112]

The manipulative and unfair techniques often used online to satisfy adolescent needs and the key features of online services that strongly meet adolescent needs have raised concerns among academics and policy makers.[113] As a result, the question has emerged whether certain data-collection practices with a potential negative impact that are directed to children, such as intrusive profiling or emotional manipulation, can be considered unfair and should be clearly prohibited in law, a question which will be discussed below.

3.4 Learning from Consumer Law: Vulnerability as a Legislative Benchmark

EU consumer law, in contrast to the data protection law, has already distinguished a special category of 'vulnerable consumers' and provided justification for their protection. Article 5(3) of the Unfair Commercial Practices Directive states: 'Commercial

[108] Giedd (2008); McAnarney (2008); McCreanor / Barnes / Gregory / Kaiwai / Borell (2005); Steinberg (2007, 2008).

[109] Giedd (2008); McAnarney (2008); McCreanor / Barnes / Gregory / Kaiwai / Borell (2005); Steinberg (2007, 2008).

[110] Preston / Crowther (2014), 454.

[111] Preston / Crowther (2014), 454.

[112] Montgomery (2015), 777.

[113] Montgomery (2015).

practices which are likely to materially distort the economic behaviour only of a clearly identifiable group of consumers who are particularly vulnerable to the practice or the underlying product because of their mental or physical infirmity, age or credulity in a way which the trader could reasonably be expected to foresee, shall be assessed from the perspective of the average member of that group.'

The Unfair Commercial Practices Directive creates a specific protection regime for vulnerable consumers as a special group because 'vulnerable consumers can be presumed to be in need of more protection than the "average consumer"'.[114] This regime provides enhanced protection departing from the general standard of consumer protection from unfair commercial practices, which is tailored to the average, 'reasonably circumspect' consumer. This approach, which Mak calls targeted differentiation, creates a criterion which follows specific needs of consumers in need of protection.[115]

This concept of vulnerability in the Unfair Commercial Practices Directive is essentially related to the personal situation of weakness in which individuals might find themselves due to their physical or demographic characteristics.[116] The European Consumer Consultative Group calls this 'the personal dimension or horizontal approach' to consumer vulnerability.[117]

Although there exists no single, universally adopted definition of consumer vulnerability, the understanding of this concept in academic literature is much broader than in the Unfair Commercial Practices Directive. In addition to the personal characteristics of the consumer, increasingly more definitions include among vulnerability factors the overall situation in which the consumers find themselves. These factors can be divided into 'endogenous' (internal) and 'exogenous' (external) factors.[118] 'Endogenous' refers to 'causes that are inherent to the consumer or his or her physical or mental situation (children, adolescents, seniors, the disabled, etc.)'.[119] They can be temporary (e.g. illness) or permanent (e.g. impairment).[120] Exogenous causes include lack of knowledge of the language, lack of general or market-specific

[114] Mak (2010), 14.

[115] Mak (2010), 13-14.

[116] For example, the European Commission recognises: '(p)romoting products which are particularly appealing to teenagers might exploit their lack of attention or reflection, as well as their risk-taking behaviour, due to their immaturity and credulity.' European Commission, Commission Staff Working Document, Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices, 25 May 2016, SWD(2016) 163 final, 45.

[117] European Consumer Consultative Group (2013).

[118] European Parliament, Report on a strategy for strengthening the rights of vulnerable consumers(2011/2272(INI)), 8 May 2012.

[119] European Parliament, Report on a strategy for strengthening the rights of vulnerable consumers(2011/2272(INI)), 8 May 2012.

[120] European Parliament, Report on a strategy for strengthening the rights of vulnerable consumers(2011/2272(INI)), 8 May 2012.

education or the need to use unknown new technologies.[121] Waddington claims that even 'the nature of the products', such as complex financial and investment products, or 'services and the selling arrangements', such as sales in combination with a free gift or special marketing practices, should count as external vulnerability factors.[122]

On the policy-making level as well, there have been calls to expand the definition of vulnerable consumers and incorporate 'situational vulnerability' or a 'sectoral approach'.[123] This approach would indeed recognise that the same consumers that in some markets are 'average consumers', i.e. reasonably well-informed, observant and circumspect, in other markets are vulnerable consumers who are not able to make informed, rational consumer choices.

Both groups of factors turn out to be important in practice. A recent empirical study on vulnerability demonstrates that the broader market environment is an important element of vulnerability, but that temporary or permanent characteristics of the consumer also play an important role.[124] Vulnerability can be both 'a permanent or long-term condition, often related to factors internal to the consumer, such as age, inexperience or a disability', and 'dynamic and relative' in its nature, arising in interaction with markets and services. Thus, any consumer can become vulnerable at times depending on his personal situation and characteristics, and on the products or services and marketing used.[125] According to the European Commission's recent interpretation of the vulnerability concept, '[V]ulnerability is not a static condition. Consumers may move in and out of states of vulnerability and they may be vulnerable in respect of some categories of transaction but not others. In addition, vulnerability is best viewed as a spectrum rather than a binary state'.[126]

A recent EU study tried to provide an evidence-based definition of consumer vulnerability that can be used to update and enhance existing vulnerability definitions. According to the study, a 'vulnerable consumer' is:

A consumer who, as a result of socio-demographic characteristics, behavioural characteristics, personal situation, or market environment:

- Is at higher risk of experiencing negative outcomes in the market;
- Has limited ability to maximise their well-being;
- Has difficulty in obtaining or assimilating information;
- Is less able to buy, choose or access suitable products; or
- Is more susceptible to certain marketing practices[127]

---

[121] European Parliament, Report on a strategy for strengthening the rights of vulnerable consumers(2011/2272(INI)), 8 May 2012.

[122] Waddington (2014).

[123] European Consumer Consultative Group (2013).

[124] European Commission, Consumer vulnerability across key markets in the European Union, Final report, January 2016.

[125] Waddington (2014).

[126] European Commission, Consumer vulnerability across key markets in the European Union, Final report, January 2016, xvii.

[127] European Commission, Consumer vulnerability across key markets in the European Union, Final report, January 2016, xx.

This definition provides a comprehensive picture of vulnerability factors and resulting negative outcomes or limitations in consumer economic behaviour. It takes into account not only the demographic characteristics, such as age, and the market environment, but also behavioural features. In relation to children the latter is an important, albeit an often disregarded factor.

Personal factors, i.e. youth and consequently inexperience, are the primary causes of vulnerability. Youth is an enduring characteristic for this group of consumers. However, it could be claimed that children can be considered more vulnerable than many other types of consumers. While many other groups of consumers change their states of vulnerability by acquiring and losing external vulnerability factors, children will often fall under both groups of internal and external vulnerability factors. Children could be permanently vulnerable consumers due to their personal situation and often vulnerable due to the characteristics of products, services and marketing techniques.

3.5 Critical Understanding and Susceptibility

From a consumer law perspective, children and teenagers may be more vulnerable as consumers not only because they lack knowledge and skills, but also because (partially due of this lack) they can be more easily influenced by others.[128]

Research on consumer socialisation deals with the development of consumer skills, knowledge and attitudes of children and adolescents.[129] It indicates that the ability to act as consumers is increasingly acquired with growth. Research on the ability to understand advertising demonstrates that younger children are not able to identify, critically assess and understand the persuasive aim of advertising.[130] From 7 to 8 years of age children start to distinguish the persuasive intent and realise that advertisements can be deceptive or biased.[131] From 11 years children become more sceptical in relation to advertisements and their intent and tactics.[132] Rozendaal et al. specifically studied the differences in cognitive advertising competencies between children (8–12 years old) and adults (18–30 years old).[133] They showed that around the age of 9–10 children become able to recognise advertising to the same extent as adults, but at age 12 children still cannot understand selling and persuasive intent of advertising equally to adults.[134] Recognition of the selling intent of advertising develops earlier than the understanding of the persuasive intent.[135] Yet these age

[128] Duivenvoorde (2013).

[129] John (2008).

[130] Martin (1997); Rozendaal / Lapierre / van Reijmersdal / Buijzen (2011).

[131] John (2008).

[132] John (2008).

[133] Rozendaal / Buijzen / Valkenburg (2010).

[134] Rozendaal / Buijzen / Valkenburg (2010).

[135] Rozendaal / Buijzen / Valkenburg (2010).

thresholds of recognising and understanding advertisements are not absolute or certain. Oates et al. claim that not all children who are 10 years old can understand the persuasive aim of advertisers.[136] Livingstone and Helsper show a more complex picture on the relationship between influence and age: 'different processes of persuasion are effective at different ages, precisely because literacy levels vary with age'.[137]

The findings on age ranges often reflect the research outcomes in the context of traditional advertising, such as on television or in newspapers, but are not to be directly transferred into the online context. Recognition of sophisticated advertising techniques in new media directed at children is much less explored than in traditional media. For example, there is only limited evidence on how children respond to embedded advertising on social media or advergames. The latter are particularly confusing due to the intrinsic intertwinement of commercial content and entertainment elements.[138] Even older children have difficulties in categorising advergames as entertainment or persuasion.[139] Their understanding even in later years of adolescence can be manipulated by advertisers through various covert techniques.[140] Product placement, host selling, branded websites and the use of celebrities all make it more difficult to understand the persuasive goal of marketing practices. A recent EU study confirms this conclusion by showing that although the most popular online games (of 25 studied games, all advergames, all social media games and half of the games provided through popular application platforms) contain embedded or contextual advertisements, children have difficulty in recognising the marketing intent of the content, in shielding themselves from it and in taking decisions.[141] The impact of imbedded advertising is considerable on children, subliminally changing their behaviour and purchasing decisions.[142]

Recent empirical data in the UK demonstrates the lack of critical understanding among children in the increasingly complex new-media landscape. Critical understanding is defined as 'a wide range of knowledge and skills, including the ability to make judgements about where information comes from and whether it is likely to be true' and 'awareness and understanding of advertising'.[143] Thus, the term describes the skills and knowledge children need to understand, question and manage online information and services. For example, only a small portion of surveyed

[136] Oates / Blades / Gunter / Don (2003), 69.

[137] Livingstone / Helsper (2006), 560.

[138] Rozendaal / Lapierre / van Reijmersdal / Buijzen (2011); Verdoodt / Clifford / Lievens (2016).

[139] Fielder / Gardner / Nairn / Pitt (2008).

[140] Fielder / Gardner / Nairn / Pitt (2008).

[141] European Commission, Study on the impact of marketing through social media, online games and mobile applications on children's behavior, March 2016.

[142] European Commission, Study on the impact of marketing through social media, online games and mobile applications on children's behavior, March 2016.

[143] OFCOM (2016).

12 to 15-year-old children are able to identify sponsored links on Google as advertising (24% of 8 to 11-year-olds and 38% of 12 to 15-year-olds).[144]

4 Combining the Safeguards of the Personal Data and Consumer Protection Regimes… Benefiting Children?

The introduction of the specific child-related rules in the GDPR brings practical challenges in relation to the implementation of well-established but age-blind data protection principles, such as fairness and transparency. For example, data controllers in practice will have to figure out how to provide information about their data-collection practices to children in a meaningful way.[145] The GDPR child-specific rules also raise conceptual questions, such as how to define an average child and delineate services directed to children. Given that consumer protection law has dealt with children as vulnerable consumers, could it inform the application of data protection in the commercial context?

The answer to this question to a large extent depends on the agreement that consumer and data protection—despite their differences—can be matched as legal frameworks.[146]

At a first glance, the combination of consumer and data protection regimes seems rather intuitive. This is due to the fact that convergence between the two regimes is already happening in practice, in EU policy making and in EU law. As outlined above, the roles of consumers and data subjects are intrinsically intertwined in the digital environment, and therefore 'the protection of consumers' personal data is an integral part of consumer protection'.[147] On the EU policy level, the interrelation between data protection, competition law, and consumer protection in the Digital Economy has become an object of discussions introduced by the European Data Protection Supervisor.[148] The proposed Digital Content Directive acknowledged that consumers actually often pay for services, not with money, but with their personal data. The GDPR explicitly referred to the Unfair Terms Directive[149] in its Recital 42 when requiring the data controllers to provide intelligible and easily accessible pre-formulated declaration of consent without unfair terms and tackled other issues that are closely related to consumer protection, such as data portability. In addition to these convergences, more generally data protection and consumer

[144] OFCOM (2016).

[145] Savirimuthu (2016).

[146] For a comprehensive discussion about the match between consumer and data protection law and its positive and difficult sides see Helberger / Borgesius / Reyna (2017).

[147] Svantesson (2017).

[148] EDPS (2014).

[149] Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (Unfair Terms Directive), OJ L 95, 21 April 1993, 29–34.

protection share many common features: they are both recognised in the Charter of Fundamental Rights of the European Union ((Article 8 (the right to data protection) and Article 38 (the consumer protection principle)),[150] both are rooted in national laws of the Member States and developed as rights starting from bottom-up secondary EU legislation.[151] Both areas of law, generally, aim to protect weaker parties (consumers, data subjects) seen as often having asymmetric information and acting in an intrinsic power imbalance.

However, the interplay between consumer protection and data protection presents many challenges and the debate about these challenges is still in its nascent phase.[152] Despite their similarities, consumer and data protection pursue different goals, especially evident in terms of interests they protect. Consumer law essentially protects economic interests of consumers by regulating their relations with product and service providers and granting specific rights to consumers in economic transactions. Data protection law, instead, protects fundamental rights of individuals and strives for fairness and lawfulness when their personal data is processed. In short, '(c)onsumer law deals with fair contracting; data protection law with fair processing'.[153] This difference in goals also leads to additional complexities. For example, some of the underlying notions, such as fairness, damages or data, are not equivalent in data protection and consumer protection law and cannot be easily matched.[154]

Finally, and most importantly, conceptually there are some fundamental obstacles for merging consumer and data protection law. One of the main normative issues stemming from the differences in scope is that combining the rules of these two policy areas arguably necessitates assumption that personal data can be treated as property and reduced to a monetary value. Yet, as claimed by Helberger et al., 'fundamental rights, such as the right to privacy and to personal data protection, which also have a societal dimension, should not be downgraded to mere individual consumer interests'.[155] Therefore, 'neither laws nor policies should fuel the idea that people can renounce their rights in exchange of services'.[156] As a result, these concerns have to be addressed, or at least clearly explicated, before fully supporting the

[150] Consumer protection is not as much fundamental substantive right at the EU primary-law level as data protection, but more a principle to be observed by public institutions, implemented through legislative or executive acts of the EU or the Member States and observed by the courts when interpreting these acts. Article 169 TFEU clearly outlines the objectives of the EU consumer protection policy: protection of the health, safety and economic interests of consumers, promotion of their right to information and education and to organization in order to safeguard their interests.

Also, consumer rights are not human rights stricto sensu, although there have been efforts to argue that consumer rights should be considered (soft) human rights. See Deutch (1994).

[151] Svantesson (2017).

[152] Svantesson (2017), Helberger / Borgesius / Reyna (2017).

[153] Helberger / Borgesius / Reyna (2017), 1427.

[154] Helberger / Borgesius / Reyna (2017), 1460.

[155] Helberger / Borgesius / Reyna (2017), 1463.

[156] Helberger / Borgesius / Reyna (2017), 1463.

extension of consumer law rationales and rules into data protection, the area of fundamental human rights where personal data is much more than a commodity.

While acknowledging the differences between consumer protection and data protection and related conceptual challenges, it cannot be denied that the combination of the two areas can be informative and potentially enhance protection of children as data subjects and consumers in the data-driven digital world. Indeed, one must acknowledge the somewhat ironically oxymoronic consequences of failing to accept the economic significance of personal data as illustrated by the motivation behind the proposed Digital Content Directive to extend consumer protections. More specifically, although the EDPS has criticised the positioning of personal data as counter-performance,[157] failing to do so also eliminates the proposed contractual protections where the only 'price' paid is personal data, thereby actually negatively impacts the data subject's consumer rights and protections. Although the EDPS has recommended alternatives to replace the use of the notion of data as counter-performance,[158] no clear solution has presented itself.

4.1 Child-Adapted Transparency

The GDPR requires data controllers to give information to all data subjects in a clear, audience-appropriate language when their personal data is collected. They are asked to adapt the information on data collection to children, as Recital 58 requires that information be given 'in such a clear and plain language that the child can easily understand'. In order to properly implement this requirement a change of mentality should happen, and data controllers should take account of the age, cognitive development, needs and abilities of the data subjects. As noted by Danoso et al.:

> it is fundamental to re-think legal documents such as Terms of Use and Privacy Policies from a perspective that better fits children's needs, their rights and their not-yet fully developed cognitive capabilities. Increasing transparency in the case of children means communicating things differently, but openly, establishing clear boundaries regarding what is allowed on the website and what is not and, above all, relating the legal content as much as possible to the children's worldviews and experiences so that it becomes truly meaningful and engaging. Children are not adults, and therefore when it comes to legal communication, they should not be treated as such.[159]

In reflecting on a possible implementation of child-adapted transparency, personalised information, symbols and participatory transparency are considered as tentative solutions below.

---

[157] EDPS (2017).

[158] In order to define the scope of the proposed Digital Content Directive without making reference to data as counter-performance, the EDPS recommended: 1) to use a broad definition of a 'service' in line with the E-commerce Directive, or 2) to refer (as the GDPR) to the offering of goods and services irrespective of whether a payment is required. EDPS (2017), 10-11.

[159] Donoso / van Mechelen / Verdoodt (2014), 54.

4.1.1 Personalised Information

Consumer protection law has been based on the assumption that information asymmetry exists between service providers and consumers and that legislative obligations imposed on providers to make specific information available could correct the imbalance.[160] Therefore, presumably, if traders provide clear, accurate and substantiated information to consumers, consumers are enabled to make informed and meaningful choices. This information-based approach constituted 'the hallmark of EU consumer law' since the 1970s.[161] However, in recent years, drawing on the insights from behavioural economics, psychology and the neurosciences, this approach relying on the rational-choice model has been challenged as being no longer effective and reflecting neither consumer behaviour nor digital reality. Reliance on the average consumer as a yardstick contradicts empirical findings, and provision of standardised information is no longer able to restore symmetry between traders and consumers.[162] Thus, '"regulating for information" is passé and the new challenge is to "regulate for rationality", or put more simply, to help consumers overcome cognitive biases that may be exploited by traders'.[163] As a consequence, alternative approaches replacing the information paradigm have been proposed, ranging from nudging[164] to personalised information disclosures.[165] The latter, invented by Busch, is particularly interesting in the case of children, although still at an early stage of academic debate. This approach proposes to use big-data analytics to provide personalised information disclosure to consumers instead of standard pre-contractual information, as currently prescribed by EU consumer law.[166]

Provision of such a personalised information theoretically looks very promising as it could take into account the specific needs, behaviour and vulnerabilities of consumers like children and tailor information to their age, personality, cognitive capacity. For example, based on past online behaviour, browsing history and demographic characteristics, algorithms could recognise a user as a child or even a child of a certain age and gender, and provide child-adapted information. The same logic and mechanism are employed by the behavioural advertising industry when serving targeted adds to the users, so could they be turned into the benefit of consumers?

Nevertheless, although promising and interesting from a consumer law perspective, personalised information as a transparency mechanism cannot be easily aligned with the core data-protection requirements. The implementation of this mechanism requires prior and potentially continuous personal data collection and profiling of

[160] Micklitz / Reisch / Hagen (2012), 272.

[161] Busch (2016).

[162] Sibony / Helleringer (2015).

[163] Sibony / Helleringer (2015), 217.

[164] Sunstein (2014); Alemanno / Sibony (2015).

[165] Busch (2016).

[166] Busch (2016).

children.[167] The GDPR allows measures based on profiling of adults with their explicit consent but limits the possibilities for profiling children, even if none of its articles explicitly states so. Recital 38 states that specific protection should apply when children's data is used for the purposes of creating personality or user profiles. Recital 71 instructs that solely automated decision-making, including profiling, with legal or similarly significant effects should not concern children. Yet recitals are not legally binding and cannot create rights and obligations that are not mentioned in the main legislative text.[168] Due to the lack of a clear position in the GDPR text, it can be debated whether the above-mentioned automated decisions are completely prohibited. The prohibition against creating personality or user profiles of children for targeted advertising purposes, for example, would be in line with the position of the Article 29 Working Party, which stated that behavioural advertising 'will be outside the scope of a child's understanding and therefore exceed the boundaries of lawful processing'.[169] Even when profiling measures in relation to children are allowed by the GDPR, Article 22 of the GDPR will be interpreted strictly and in favour of children, for example, when deciding what decisions might have a significant effect on children.[170]

Nevertheless, in relation to personalised information as a transparency tool, it is questionable whether measures involving automated decisions based on profiling that aim to benefit children and enhance their rights, i.e. have no significant (negative) effect, should be allowed. If such measures were considered in line with the GDPR, what would be the legal ground for the related data processing? Would children be asked for explicit consent to be profiled, can such consent be informed and if so, at what age? If commercial profiling is allowed, even if for supposedly positive purposes, what additional safeguards can guarantee that the major problems associated with profiling, such as the lack of control over the profile, its possible use and abuse or opaque steering of consumer choices,[171] are accounted for?

4.1.2 Information in Symbols

The Consumer Rights Directive requires that information be provided in a 'clear and comprehensible manner'. The recitals of the Directive take particular account of vulnerable consumers, stating that the trader should take into consideration 'the

[167] In addition to the disproportionate data collection and processing, the EDPS also noted the following potential problem related to the automatic systems that infer the age of a user from his or her behavior: 'false identification of the age of the user under such behavioural analysis systems, particularly with respect to children who have a wide spectrum of maturity and behaviours as they grow and develop'. EDPS (2012), 7-8.

[168] Mendoza / Bygrave (2017).

[169] Article 29 Data Protection Working Party, Opinion 02/2013 on Apps on Smart Devices, WP 202, 27 February 2013, 26. See also Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioral advertising, WP 171, 22 June 2010.

[170] Mendoza / Bygrave (2017).

[171] Van der Hof / Prins (2008); Hildebrandt (2008).

specific needs of consumers who are particularly vulnerable because of their mental, physical or psychological infirmity, age or credulity in a way which the trader could reasonably be expected to foresee' (Recital 34). Not only the content of information is important, but also its presentation and visualisation.[172] Legal information for users should not only be as clear as possible, but also accessible and engaging. In fact, 'multi-layered' privacy notices[173] or visceral notices[174] have been proposed to improve the understanding and readability of information provided to the users. Visceral notices use intuitive, familiar visual signals in order to show consumers, instead of telling them, when their data is collected.

Although the GDPR has made its first steps in using symbols to improve transparency, icons have long been used in various sectors to inform consumers about products. Online digital products are not an exception, as the Guidance on the Consumer Rights Directive refers to the use of icons to provide information to consumers in a uniform and comparable way.[175] Its Annex I provides a set of icons to illustrate the relevant information categories, such as model for the display of consumer pre-contractual information about online digital products in accordance with Article 8(2) and (4) of the Consumer Rights Directive. It encourages traders to use the information categories with their icons. Yet, the benefits of presenting pre-contractual information, as required under the Consumer Rights Directive, in the form of icons are uncertain. The findings of a recent behavioural study suggest that the presence of icons hardly affects the use of pre-contractual information and does not facilitate (and in some cases even lower) understanding of the information among adult consumers.[176] As a result, it has been concluded that a compulsory use of model forms with icons is not recommended but there may be merits in promoting icons on a voluntary basis for specific sectors and product categories, for example under the self and co-regulation developed by traders.[177]

The GDPR also mentions the use of standardised icons as easily visible and intuitive symbols for conveying privacy policies to the Internet users. Nevertheless, in the adopted text of the Regulation there is no effort to compose a list of such privacy icons. The European Parliament in its first reading provided a provisional list of icons and related particulars.[178] However, the list has been abandoned in the

[172] John / Acquisti / Loewenstein (2009).

[173] Article 29 Working Party, Opinion 10/2004 on more harmonised information provisions, WP 100; Noain-Sánchez (2015).

[174] Calo (2012), 1033.

[175] European Commission, Guidance Document concerning Directive 2011/83/EU.

[176] European Commission, Consumer Market Study to support the Fitness Check of EU consumer and marketing law, May 2017.

[177] European Commission, Study on the application of the Consumer Rights Directive 2011/83/EU, May 2017.

[178] European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 –C7-0025/2012 –2012/0011(COD)), P7_TA(2014)0212.

further GDPR adoption process and in practice has turned out to be controversial as to its comprehensiveness. This is not surprising, given that 'privacy safeguards are not easily reduced to metrics as are vitamins and calories on a nutritional label or miles per gallon on an auto sticker'.[179] In fact, research shows that representing privacy in icons is difficult, the icons are not always noticed by the users and the users need to learn the meaning of the icons, thus, user education is necessary in parallel.[180] Various icons have been developed by industry and academics, but their success has been limited.[181] For example, the AdChoices icon adopted by the online advertising industry has been seen as a failure as users had major troubles in understanding it.[182] However, it is also recognised that standard information mechanisms are necessary—although if used alone they are not sufficient—as such mechanisms help to find information more quickly and facilitate comparison among products and services.[183] For example, research found that a privacy "nutrition label"—a label inspired by actual nutrition labels used in food production—helped users to get information more accurately and quickly compared to traditional privacy policies.[184] Even if promising in research, this label has not yet been widely adopted in practice.

It is debatable if and to which extent icons, pictograms and other non-verbal ways of transmitting information can be effective and feasible for the implementation of the GDPR. In the light of empirical findings, it has been claimed that icons could provide a more intuitive and easy to read privacy notices for children but traditional notices should remain available at the same time.[185] Indeed, the design and layout of visual notices, that might include not only images, icons but also text or the combination of all these elements, can influence users' attention and comprehension of the notice.[186] As younger children are less able to compare and select products and to deal with huge amounts of information when making decisions,[187] icons might turn out to be useful to them in finding and comparing information.

Notwithstanding the lack of effective solutions, the experience of consumer law can be inspirational for data protection law. For example, learning about the problems that the icons related to pre-contractual information about online digital products under the Consumer Rights Directive face could allow avoiding the same

[179] Electronic Privacy Information Center (2012).

[180] Schaub / Balebako / Durity / Cranor (2015).

[181] See e.g., Disconnect Privacy Icons (available at: https://disconnect.me/icons) or A. Raskin's Privacy icons (available at: http://www.azarask.in/blog/post/privacy-icons/); Holtz / Zwingelberg / Hansen (2011).

[182] Leon / Cranshaw / Cranor / Graves / Hastak / Ur / Xu (2012).

[183] Cranor (2012).

[184] A privacy 'nutrition label' summarises main elements from a privacy policy in a standard form. See Kelley / Cesca / Bresee / Cranor (2010).

[185] Mantelero (2016).

[186] Choe / Jung / Lee / Fisher (2013); Schaub / Balebako / Durity / Cranor (2015).

[187] John / Cole (1986).

mistakes in data protection or help framing discussions about where changes are needed.

In the interim however not only the effectiveness of visual mechanisms to convey information to individuals should be increased but also adequate incentives should be put in place for the developed solutions to be adopted and enforced. Such an approach might better align the mismatch between the positive results in academic research versus the complete failure of self-regulatory transparency mechanism, such as the AdChoices icon. Moreover, definitive transparency mechanisms developed in collaboration with data protection authorities could create industry standards and common icons facilitating data subject awareness and allowing for the recognition of iconographic meaning.

4.1.3 Participatory Transparency

Even in child-adapted and easily readable or visualised privacy policies several discrepancies among users might remain, especially 'a gap between what users assume the terms contain and what they actually say' and the thinking among the users that terms and policies 'are there to protect them rather than consisting of a contract with legal obligations and duties'.[188] Empirical data on children demonstrates the existence of these cognitive biases. For example, 68% of Canadian children think that 'if a website has a privacy policy, that means it will not share my personal information with others'.[189] Similarly, in Italy many adolescents consider that 'the mere existence of a published privacy policy is *per se* sufficient to guarantee an adequate level of protection'.[190]

Instead of trusting that service providers will adapt their complex and legalese privacy policies to particular users and help to overcome the above-mentioned biases, user education and participation seems to be key in order to enhance transparency. Dreyer and Ziebarth propose relying on direct user engagement to improve transparency and readability of information that social-media services and platforms provide to their users.[191] More specifically, they suggest the participatory transparency approach, i.e. 'the use of autonomous bodies of third-party users to crowd-source platform-specific suggestions for improvements, and to translate terms and provisions into practical pointers'.[192]

The participatory transparency approach enables users to become active in explaining and transferring knowledge on the privacy policies and the terms of use to other users instead of being passive information receivers. In concrete terms, according to this approach, users can be organised in different forms ranging from

[188] Dreyer / Ziebarth (2014), 532.

[189] Steeves (2014a).

[190] Mantelero (2016), 174.

[191] Dreyer / Ziebarth (2014).

[192] Dreyer / Ziebarth (2014), 529.

formally institutionalised user boards and councils to informal forum and action groups. They are envisioned to contribute to the terms of use and privacy policies by unravelling their content and consequences, identifying problematic aspects and cognitive biases, demonstrating illegible and unclear provisions, aligning provisions with user expectations and social norms and providing crowd-sourced suggestions for improvements.[193] As proposed by Donoso et al., concrete mechanisms to realise this idea could be, for example, 'providing an *'idea-box'* for children to send suggestions about new (examples of) rules or agreements, or modifications to existing ones' or 'to develop a sort of "crowd-sourcing" feature where children can actively interact, discuss, propose and eventually vote on current and new rules'.[194]

The participatory transparency approach would not only make privacy policies of digital services and products more comprehensive, increase user awareness and possibly lead to improvements, but would also be aligned with the child-rights perspective. It would enable children to be heard and respect their rights to participate and express their views freely in all matters affecting them, as enshrined in Article 12 of the UN Convention on the Rights of the Child. Child participation means 'ongoing processes, which include information-sharing and dialogue between children and adults based on mutual respect, and in which children can learn how their views and those of adults are taken into account and shape the outcome of such processes'.[195] Meaningful participation and representation of children as Internet users can demonstrate their perspectives and values and contribute to the design of the rules that better resonate with children's viewpoints.

Improvement of transparency through the involvement of children has been used by scholars[196] and public institutions[197] studying the readability and comprehensibility of privacy policies within groups of children and exploring online privacy and transparency through youth juries.[198] Children's participation has proved to be particularly useful in identifying transparency issues, testing child-adapted privacy policies and deliberating and transferring knowledge about their implications.

4.2 Fairness

In addition to the duty of providing information to individuals, both data-protection and consumer protection law rely on the principle of fairness. Although it is challenging to combine the notions of fairness in both fields due to the potential

[193] Dreyer / Ziebarth (2014), 529.

[194] Donoso / van Mechelen / Verdoodt (2014), 54.

[195] UN Committee on the Rights of the Child, *General Comment No. 12: The Right of the Child to be Heard*, UN Doc. CRC/C/GC/12, 20 July 2009.

[196] Micheti / Burkell / Steeves (2010); Donoso / van Mechelen / Verdoodt (2014).

[197] UK Children's Commissioner (2017).

[198] Coleman / Pothong / Perez Vallejos / Koene (2017).

differences in their scope and meaning, this is a necessary analysis in order to facilitate the alignment of these respective policy agendas.

4.2.1 Fairness in Data Protection

The GDPR, like its predecessor Directive 95/46/EC, requires data controllers to process personal data fairly. This principle generally enjoys a broad interpretation and means that personal data should be processed in a transparent way, i.e. data controllers are clear and open with data subjects about how and why their information will be collected and used. Besides transparent information, some interpret fairness as additionally requiring that personal data be handled only in ways individuals would reasonably expect, and most importantly, that personal data not be used in ways that unjustifiably cause a negative impact on individuals.[199] Bygrave claims: 'at a very general level, the notion of fairness undoubtedly means that, in striving to achieve their data-processing goals, data controllers must take account of the interests and reasonable expectations of data subjects; controllers cannot ride roughshod over the latter.'[200] There is a consensus among data protection authorities that 'any processing of personal data that gives rise to unlawful or arbitrary discrimination against the data subject shall be deemed unfair'.[201]

Several authors have distinguished this broad role for fairness noting implicit and explicit meanings of the term. In particular, explicit fairness here strongly refers to transparency with implicit fairness relating instead to the balancing of interests and the reasonable expectations of the data subject.[202] In commenting on this division, Clifford and Ausloos instead propose a distinction between procedural fairness and fair balancing, given the modifications introduced by the GDPR in relation to fairness.[203] In short, the authors suggest a procedural fairness element composed of three components (namely transparency, timeliness and the burden of care) given the role played by data controllers in the implementation of the requirements.[204] In addition to this, the fair balancing elements relate to the principles of proportionality and necessity and their application to the balancing of the rights and interests in the context of the given circumstances.[205]

Due to the broadness of the overarching principle of fairness it is difficult to understand its precise meaning. As such, it is arguable that this principle could be informed by the fairness principle in consumer protection law (as contained in the Unfair Terms and Unfair Commercial Practices Directives).

---

[199] ICO, the Guide to Data Protection (2016).

[200] Bygrave (2002), 58.

[201] International Conference of Data Protection and Privacy Commissioners (2009).

[202] Bygrave (2002); Clifford / Ausloos (2017).

[203] Clifford / Ausloos (2017).

[204] Clifford / Ausloos (2017).

[205] Clifford / Ausloos (2017).

4.2.2 Consumer Protection and Fair Data Gathering and Use

Given that data protection is an omnibus regime, in consumer protection law the principle of fairness is more specific as it is restricted to the commercial business-to-consumer context. Fairness in consumer law refers not only to transparent contractual information, but also to the way in which a consumer is persuaded to agree to the contractual clauses and to the content of the clauses themselves. In short, there are two clear manifestations in fairness, namely: (1) the Unfair Terms Directive and (2) the Unfair Commercial Practices Directive.

The Unfair Terms Directive qualifies a non-negotiated term in a contract or a consent statement as unfair if, 'contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer'.[206] Therefore, all contractual clauses are taken into account in determining unfairness, not limited to those related to the processing of personal data.[207]

The fairness test in the Unfair Terms Directive could be used to evaluate the fairness of terms and conditions related to personal data (e.g. excessive data collection, unlimited data sharing with the third parties) and the fairness of the position of the consumer in a commercial context. The fairness of contractual clauses could also be assessed using data protection requirements as an assessment criteria, e.g. a contract could be considered unfair if it violates data minimisation, security or data protection by default requirements.[208]

Consumer organisations have already referred to consumer law to test the fairness of the terms and conditions of companies collecting personal data. A recent example is an action which combined data protection and consumer protection to scrutinise the terms of use and privacy notices of connected toys.[209] Also in the context of social networks, the Unfair Term Directive has been applied to all types of contracts between consumers and businesses by the Consumer Protection Cooperation Network.[210]

Furthermore, the Unfair Commercial Practices Directive protects consumers from unfair commercial practices, i.e. any conduct by a trader directly connected with the promotion, sale or supply of a product, 'before, during and after a commercial transaction in relation to a product'.[211] As noted by Helberger et al., given that consent to personal data processing can be considered a transactional decision, the Unfair Commercial Practices Directive 'could help to assess the fairness of the conditions under which users are required to agree to the collection and use of their

[206] Article 3 of the Unfair Terms Directive.

[207] Wauters / Lievens / Valcke (2013), 64.

[208] Helberger / Borgesius / Reyna (2017), 1451.

[209] Forbrukerrådet (the Norwegian Consumer Council) (2016).

[210] Consumer Protection Cooperation Network (2017), 3.

[211] Article 2(k) and 3 of the Unfair Commercial Practices Directive.

personal data – e.g. take-it-or-leave-it choices, misinforming about the functionality of the service if consumers do not agree, etc.'[212]

A practice is unfair if it is 'contrary to the requirements of professional diligence and materially distorts or is likely materially to distort the economic behaviour of the average consumer with regard to the product'.[213] Data processing practices that might have a detrimental effect on the average data subject, therefore, could be considered as violating the Unfair Commercial Practices Directive's fairness principle even if the data subject consented to them.

The use of consumer fairness test could have potential benefits for children and allow assessing them in the light of children's vulnerability to the practice or the underlying product. As outlined before, due to specific characteristics, needs and preferences children might be particularly vulnerable as consumers. For example, it has been argued that the use of certain techniques such as advergames can have a manipulative effect with such techniques often implementing personal data gathering as part of the commercial offering.[214] Given the gamification of the personal data collection it is arguable that such a technique could fall foul of the fairness test in the Unfair Commercial Practices Directive. Interestingly, it is also questionable whether advergames themselves (i.e. aside from the data gathering aspects) may be in breach of the Unfair Commercial Practices Directive's fairness test due to the manner in which they integrate commercial and non-commercial content combined with the capacity to personalise such content.

Indeed, using personalised marketing 'companies could automatically adapt advertisements to (inferred) characteristics, biases and weaknesses of individual consumers'.[215] Thus, children's characteristics can be exploited by companies, taking advantage of their developmental features and manipulating their behaviour and decisions. A recent example of such manipulation is Facebook's ability to exploit emotional vulnerability of teenagers as allegedly 'the company can monitor posts and photos in real time to determine when young people feel "stressed", "defeated", "overwhelmed", "anxious", "nervous", "stupid", "silly", "useless" and a "failure"'[216] and allow advertisers to target ads accordingly.

Consumer law and its fairness principle could potentially address this concern. Relying on consumer protection, the GDPR could be interpreted as forbidding a priori some unfair and undesirable data collection and use (e.g. personalisation) practices. Consumer law would also allow to establish violation of fairness even in cases where the child or his representative has consented to the processing. In addition, the blacklist contained in Annex 1 in the Unfair Commercial Practices Directive could be updated to include a list of unfair commercial data-processing practices in

[212] Helberger / Borgesius / Reyna (2017), 1545.

[213] Articles 5(2) and 6(1) (a) of the Unfair Commercial Practices Directive.

[214] Verdoodt / Clifford / Lievens (2016).

[215] Helberger / Borgesius / Reyna (2017), 1458.

[216] The Guardian, Facebook told advertisers it can identify teens feeling 'insecure' and 'worthless', 1 May 2017.

order to ban them as misleading or aggressive, taking into account the aggressiveness, particular characteristics of children of differing age groups and the context. This would be in line with the thinking which has developed in the US after almost two decades of the Children's Online Privacy Protection Act (COPPA) experience. Montgomery and Chester argue that some collection practices of children's data, such as profiling, behavioral advertising, cross-platform tracking and geolocation targeting should not be allowed by law even with parental permission.[217]

Yet, the impact of these suggestions should be carefully considered in light of the UN Convention on the Rights of the Child, which in addition to protection provide children with strong claims related to participation and provision.[218] A blunt prohibition of specific data collection practices could be viewed as overprotection for older children, who (if properly informed) might be increasingly able to decide for themselves to consent to such practices or not. However, the limitations and shortcomings of consent are widely acknowledged in relation to adults, let alone children.[219] Also, many data processing practices might not be easily classified as having a purely negative effect and might in parallel bring some benefits for a child, which can easily be curtailed by taking too paternalistic approach. Despite this, one must acknowledge that the very purpose of many of these practices is to manipulate.

Therefore, reliance on fairness as it is understood in consumer protection law could allow data protection to shift the focus from procedural safeguards (e.g. parental consent to data processing) to a fundamental and comprehensive assessment of data processing practices and terms as fair.[220]

4.3 Services Offered Directly to Children

The GDPR requires parental consent when online services are offered directly to children under the age of 16 (unless national laws specify a lower age threshold between 13 and 16). However, websites with mixed audiences rather than services created for children are the ones to generate major privacy concerns and anxieties. Various studies in Europe[221] and North America[222] report that from a broad range of websites that children nowadays use, the most favorite websites are often not directed to or targeting children (at least not those under 13), such as YouTube, Facebook and Google. Many of these websites claim in their terms of use that their services are not intended for those under 13, even if in practice young children are

[217] Montgomery / Chester (2015).

[218] Article 12 (the right to be heard) and Article 17 (the right to have access to media) of the UN Convention on the Rights of the Child.

[219] Van der Hof (2016).

[220] On the limits of protection offered to children under the rules on children's consent in the EU see Van der Hof (2016).

[221] Livingstone / Haddon / Görzig / Ólafsson (2011).

[222] Steeves (2014b).

active there in substantive numbers. It is well documented that services not directed or clearly appealing to children, e.g. contain no cartoon characters, are used by children.[223]

Due to the very recent GDPR adoption, at the time of writing, there has not been an official guidance at the EU level on the extent that the parental-consent requirement will cover general-audience or mixed-audience services and sites. Therefore, many uncertainties and questions remain: How to delineate information-society services offered directly to a child from general-audience services? How many children should the service have among its users to be covered by the GDPR parental-consent requirement, i.e. what if it does not target children as its primary audience? When, if at all, does the GDPR apply to mixed-audience websites? Do data controllers need to have 'actual knowledge' that children are providing them with personal data?[224]

The Unfair Commercial Practices Directive entails a similar difficulty to distinguish commercial practices directed at children from those directed at other consumers[225] and could become a useful reference in the GDPR implementation process. In order to decide whether a commercial practice is directed at children, the European Commission requires a case-by-case assessment, which should not be limited to the trader's target-group definition.[226]

In interpreting the application of Article 5(3) and (5) and point No. 28 of Annex I to the Unfair Commercial Practices Directive to games, the European national consumer protection authorities, acting through the Consumer Protection Cooperation (CPC) Network, took the position that the Unfair Commercial Practices Directive applies not only to games 'solely or specifically targeted at children', but

[223] Consumer Protection Cooperation Network (2013).

[224] The Federal Trade Commission (FTC) under the COPPA in the US takes into account the following for determining whether a website or an online service is directed at children: subject matter of the site, its visual content, the use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the website or online service, or whether advertising promoting or appearing on the website or online service is directed to children. A service will not be considered by the FTC to be directed to children if it does not target children as its primary audience and employs a filter ensuring that personal information from users is not collected prior to ascertaining their age, and consequently prevents the collection of personal information from individuals who have stated they are younger than 13. See FTC, A Guide for Business and Parents and Small Entity Compliance Guide, available at: https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.

[225] It can be difficult to distinguish marketing directed at children from marketing directed at other consumers in the context of the banned commercial practice 28 in Annex 1 (direct exhortations to children) of the Unfair Commercial Practices Directive. European Commission, Commission Staff Working Document, Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices, 25 May 2016, SWD(2016) 163 final.

[226] European Commission, Commission Staff Working Document, Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices, 25 May 2016, SWD(2016) 163 final.

also to games that are 'likely to appeal to children'.[227] The trader should be reasonably able to foresee that his service is likely to appeal to children.[228]

In addition, national authorities have adopted criteria to determine whether services are likely to appeal to children. For example, in the context of online games the UK Office of Fair Trading considers 'whether children are known to play the game' and 'if the game is marketed to children' as two determining factors and establishes the following open list of criteria related to the content, style and presentation of the game: characters popular with children, cartoon-like graphics, bright colours, simplistic language, activity appealing to or popular among children, no age restriction for downloading, availability in the child section in an app store.[229]

The guidance for data controllers on the definition of information-society services offered directly to a child could take into account the Unfair Commercial Practices Directive's interpretation of commercial practices directed at children and thus include not only services that are clearly targeted at children, such as e.g. YouTube Kids, but also services that are likely to appeal to children. The latter criterion could be defined considering the specific characteristics (the content, style and presentation) of services and the fact that services are actually used by children (based on e.g. empirical evidence on audience composition), even if the service provider employs a different target-group definition. Furthermore, in some cases consumer protection law could become instrumental in deciding if information society services are offered directly to children. If, according to the Unfair Commercial Practices Directive, an advertising promoting or displayed on the website or service, was directed at children, the whole information-society service could be considered as being offered directly to children under the GDPR.

4.4 Defining an Average Child

When a commercial practice is specifically aimed at a particular group of consumers, such as children, the Unfair Commercial Practices Directive advises that the impact of the commercial practice be assessed from the perspective of the average member of that group. The average-consumer standard, although criticised as imprecise and ambiguous,[230] is dynamic. National courts and authorities have to

[227] Consumer Protection Cooperation Network (2013), 2. (It states: '*As to whether an application or a game can be considered to be directed at children within the meaning of Annex I Nr 28, the UCPD (Unfair Commercial Practices Directive) gives no clear indication. Other provisions in the UCPD contain useful criteria which can be used mutatis mutandis to address this matter. For example, Article 5(2)(b) refers to the distortion by a practice of the economic behaviour of the consumer whom it "reaches". Similarly, under Article 5(3), where a clearly identifiable group of consumers is particularly vulnerable to a practice in a way which the trader could reasonably be expected to foresee, the practice shall be assessed from the average member of that group.*').

[228] Consumer Protection Cooperation Network (2013), 2.

[229] Office of Fair Trading (2014).

[230] Incardona / Poncibò (2007), 21.

exercise their own discretion and judgment and determine the typical reaction of the average consumer in a particular case. According to Mak, 'the "unfair" character of advertising is determined on the basis of consumer perception' and the risk of 'consumer confusion' is a touchstone for the applicability of the Unfair Commercial Practices Directive.[231]

If a commercial practice is targeting a group of consumers who are less than averagely informed and circumspect, the average member of that group (rather than the average consumer in general) should be taken as the standard of assessment. For example, in advertising for children, the consumers addressed are potentially less critical and less knowledgeable of influencing practices, leading to a stricter evaluation of the advertising involved.[232]

The Unfair Commercial Practices Directive implicitly requires examining the age of the group of children targeted by the commercial practice, and determining whether this age group is vulnerable to the practice at hand. The GDPR also relies on an average-child criteria when providing protection to children as data subjects through parental consent. However, instead of evaluating an average child of a particular targeted age group, the GDPR chooses to set an age when children can be deemed competent to consent to the processing of their personal data. Such a legislative choice of determining a prescribed age limit does not account for particular age groups, their vulnerability to the particular data-collection practice or their perception.

Data-protection law could therefore define an average child in different data-collection scenarios based on comprehensive research and solid empirical evidence. As it seems highly unlikely that fixing a single age limit for consent in all data-processing activities online could be the most appropriate solution, different sectors, data-collection practices and age spans might require detailed examination and research.

Following the logic of the Unfair Commercial Practices Directive, the GDPR could start searching for an average data subject among children and explore the correlation between the characteristics of certain age groups of children and their likelihood of being vulnerable for specific commercial data-collection practices.[233]

5 Conclusions

When trying to solve the new data-protection challenges pertaining to the child-specific protection regime of the GDPR, the EU data-protection law should not try to invent the wheel but combine its efforts with consumer protection law. A holistic view on the rationale and particular provisions of both fields would not only provide inspiration from consumer law, which has been dealing with children as vulnerable

[231] Mak (2010).

[232] Duivenvoorde (2013).

[233] Stuyck / Terryn / van Dyck (2006).

consumers for some time, but also reflect the dual role of data subjects and consumers that children today play online.

In the GDPR, children, as a specific group of data subjects, are considered separately from adults because of their possible lower awareness of risks, consequences, safeguards and rights in relation to the processing of personal data online. However, the need for more protection stems from various additional factors which did not evidently motivate the European Commission. This chapter aims to broaden the understanding of the normative justifications for establishing a specific, child-tailored two-tiered data protection regime. It has showed that EU consumer protection law portrays children as vulnerable consumers due to their possible susceptibility to advertising and manipulation by traders and marketers. Both internal (e.g. age) and external (e.g. complex products and data-driven markets) elements contribute to such vulnerability. Not less important are specific interests of persons who have not yet reached physical, psychological and intellectual maturity and need to freely develop into adults. Developmental psychology underlines specific developmental features, such as emotional volatility and impulsiveness, need of identity and autonomy formation that can increase the possibility of online victimisation and commercial exploitation of personal data among children.

The chapter has also demonstrated that the GDPR can learn from consumer law in implementing child-adapted transparency, for example through participatory transparency and symbols, and broadening the understanding of the fairness principle and as a result banning data collection practices that are contrary to good faith and might have detrimental effects on children as data subjects. Consumer law can provide guidance on how to interpret the definition of information-society services offered directly to a child, making it possible to include not only services directly targeting children but also those that are likely to appeal to children due to their content, style and presentation. Finally, following the logic of the Unfair Commercial Practices Directive, the GDPR could rely on an average data subject, define an average child in different data collection scenarios and explore the correlation between the characteristics of certain age groups of children and their likelihood of being vulnerable to specific commercial data processing practices.

Acknowledgements The author would like to thank prof. Vanessa Mak and Damian Clifford for their helpful comments and suggestions on an earlier draft of this chapter. Any errors or omissions remain the responsibility of the author.

References

Acar, G. / Eubank, C. / Englehardt, S. / Juarez, M. / Narayanan, A. / Diaz, C. (2014), The Web Never Forgets: Persistent Tracking Mechanisms in the Wild, In Proceedings of CCS 2014, available at: https://securehomes.esat.kuleuven.be/~gacar/persistent/the_web_never_forgets.pdf

Alemanno, A. / Sibony, A. L. (2015), Nudge and the Law: a European Perspective, Hart Publishing

Blieszner, R. / Roberto, K. A. (2004), Friendship across the life span: reciprocity in individual and relationship development, in: F. R. Lang / K. L. Fingerman (Eds.), Growing together: personal relationships across the lifespan, 159, Cambridge University Press

Boneva, B. S. / Quinn, A. / Kraut, R.E. / Kiesler, S., / Shklovski, I. (2006), Teenage communication in the instant messaging era, in: R. Kraut / M. Brynin / S. Kiesler (Eds.) Computers, phones, and the Internet: Domesticating information technology, 201, Oxford University Press

Boulay, J. / de Faultrier, B. / Feenstra, F. / Muzellec, L. (2014), When children express their preferences regarding sales channels: Online or offline or online and offline?, 42 (11/12) International Journal of Retail & Distribution Management 1018

boyd, d. (2008), Taken out of context: American teen sociality in networked publics. PhD thesis, University of California

Bradshaw, S. / Millard, C. / Walden, I. (2011), Contracts for clouds: Comparison and analysis of the terms and conditions of cloud computing services, 19 International Journal of Law and Information Technology 187

Brown, B. B. (1990), Peer groups and peer cultures, in S. S. Feldman / G. R. Elliott (Eds.) At the threshold: The developing adolescent, 171, Harvard University Press

Buckingham, D. (2000). After the Death of Childhood, Cambridge, Polity

Busch, C. (2016). The Future of Pre-Contractual Information Duties: From Behavioural Insights to Big Data, in: C. Twigg-Flesner, T. (Ed.), Research Handbook on EU Consumer and Contract Law, 221, Edward Elgar Publishing

Bygrave, L. A. (2002), Data Protection Law: Approaching its Rationale, Logic and Limits, Kluwer International

Calo, R. (2012), Against Notice Skepticism In Privacy (And Elsewhere), 87 Notre Dame Law Review 1027

Choe, E. / Jung, J. / Lee, B. / Fisher K (2013), Nudging people away from privacy-invasive mobile apps through visual framing, In Proc.INTERACT'13, Springer

Clifford, D. / Ausloos, J. (2017), Data Protection and the Role of Fairness, CiTiP Working Paper 29/2017, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3013139

Clifford, D. / Van Der Sype, Y. S. (2016), Online dispute resolution: Settling data protection disputes in a digital world of customers, Computer 32(2) Law & Security Review 272

Coleman, S. / Pothong, K. / Perez Vallejos, E. / Koene, A. (2017), Internet On Our Own Terms: How Children and Young People Deliberated About Their Digital Rights, available at: http://casma.wp.horizon.ac.uk/casma-projects/5rights-youth-juries/the-internet-on-our-own-terms/

Cranor, L. F. (2012), Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice, 10(2) Journal on Telecommunications and High Technology Law 307

Deutch, S. (1994), Are consumer rights human rights?, 32(3) Osgoode Hall Law Journal 537

Donoso, V. / van Mechelen, M. / Verdoodt, V. (2014), Increasing User Empowerment through Participatory and Co-design Methodologies, Emsoc project deliverable D1.3.1c, available at: http://emsoc.be/wp-content/uploads/2014/09/D1.3.1c_ICRI1.pdf

Dowty, T. / Korff, D. (2009), Protecting the virtual child – the law and children's consent to sharing personal data, Study prepared for ARCH (Action on Rights for Children) and the Nuffield Foundation, available at: http://www.nuffieldfoundation.org/sites/default/files/Protecting%20the%20virtual%20child.pdf

Dreyer S. / Ziebarth L. (2014), Participatory Transparency in Social Media Governance: Combining Two Good Practices, 4 Journal of Information Policy 529

Duivenvoorde, B. (2013), The protection of vulnerable consumers under the Unfair Commercial Practices Directive, 2 Zeitschrift für Europäisches Unternehmens- und Verbraucherrecht 69

Erikson, E. H. (1959), Identity and the life cycle. Norton

Erikson, E. H. (1968), Identity: youth and crisis. Norton

Fielder, A. / Gardner, W. / Nairn, A. / Pitt, J. (2008), Fair Game? Assessing commercial activity on children's favourite websites and online environments, UK National Consumer Council

Garrie, D. B. / Duffy-Lewis, M. / Wong, R. / Gillespie, R. L. (2010), Data Protection: the Challenges Facing Social Networking, 6 Brigham International Law and Management Review 127

Giedd, J. N. (2008), The Teen Brain: Insights from neuroimaging, 42 Journal of Adolescent Health 335

Greenfield, P. M. / Gross, E. F. / Subrahmanyam, K. / Suzuki, L. K. / Tynes, B. (2006), Teens on the Internet: Interpersonal connection, identity, and information, in: R. Kraut (Ed.), Information technology at home, 185, Oxford University Press

Grimes, S. M. (2013), Persistent and emerging questions about the use of end-user licence agreements in children's online games and virtual worlds, 46 UBC Law Review 681

Grimes, S. M. (2015), Playing by the Market Rules: Promotional Priorities and Commercialization in Children's Virtual Worlds, 15 Journal of Consumer Culture 110

Hartup, W. W. / Stevens, N. (1999), Friendships and adaptation across the life span, 8(3) Current Directions in Psychological Science 76

Helberger, N. / Borgesius, F. Z. / Reyna, A. (2017), The perfect match? A closer look at the relationship between EU consumer law and data protection law, 54(5) Common Market Law Review 1427

Helberger, N. / Guibault, L. / Loos, M. / Mak, C. / Pessers L., Van der Sloot, B. (2013), Digital Consumers and the Law. Towards a Cohesive European Framework, Kluwer Law International

Helberger, N. / Van Hoboken, J. (2010), Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers, 4 Computer Law International 101

Helsper, E. J. / Eynon, R. (2010), Digital natives: where is the evidence?, 36 British Educational Research Journal 503

Hildebrandt, M. (2008), Defining Profiling: A New Type of Knowledge?, in: M. Hildebrandt / S. Gutwirth (Eds.), Profiling the European citizen Cross-disciplinary perspectives, 17, Springer Science

Holtz, L. E. / Zwingelberg, H. / Hansen, M. (2011), Privacy Policy Icons, in: J. Camenisch, S. Fischer-Hübner, K. Rannenberg (Eds.) Privacy and Identity Management for Life, 279, Springer

Hoofnagle, C. J. / Whittington, J. (2016), The Price of 'Free': Accounting for the Cost of the Internet's Most Popular Price, 61 UCLA Law Review 606

Incardona, R. / Poncibò, C. (2007), The average consumer, the Unfair Commercial Practices Directive, and the cognitive revolution, 30 Journal of Consumer Policy 21

John, L. / Acquisti, A. / Loewenstein, G. (2009), The Best of Strangers: Context Dependent Willingness to Divulge Personal Information, available at: http://ssrn.com/abstract=1430482

John, R. D. (2008), Stages of consumer socialization, in: C. P. Haugtvedt / P. Herr / F. R. Kardes (Eds.), Handbook of consumer psychology, 219, Taylor & Francis

John, R. D. / Cole, C. A. (1986), Age Differences in Information Processing: Understanding Deficits in Young and Elderly Consumers, 13 Journal of Consumer Research 297

Jones, C. / Shao, B. (2011), The net generation and digital natives: implications for higher education, Higher Education Academy

Jones, L. M. / Mitchell, K.J. / Walsh, W. A. (2013), Evaluation of Internet Child Safety Materials Used by ICAC Task Forces in School and Community Settings: NIJ Evaluation Final Technical Report

Kelley P. G. / Cesca, L. / Bresee, J. / Cranor L. F. (2010), Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach, CYLAB, available at: http://www.cylab.cmu.edu/research/techreports/2009/tr-cylab09014.html

Leczykiewicz, D. / Weatherill, S. (2016), The Images of the Consumer in EU Law: Legislation, Free Movement and Competition Law, Hart Publishing

Leon, P. G. / Cranshaw, J. / Cranor, L. F. / Graves, J. / Hastak, M. / Ur, B. / Xu, G. (2012), What do online behavioral advertising privacy disclosures communicate to users?, In Proc.WPES'12. ACM

Livingstone S. / Helsper, E. J. (2006), Does advertising literacy mediate the effects of advertising on children? A critical examination of two linked research literatures in relation to obesity and food choice', 56(3) Journal of Communication 560

Livingstone, S. / Carr, J. / Byrne, J. (2015), One in Three: Internet Governance and Children's Rights, Global Commission on Internet Governance Paper Series No. 22, Centre for International Governance Innovation

Livingstone, S. / Haddon, L. / Görzig, A. / Ólafsson, K. (2011), Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries, EU Kids Online, Deliverable D4, EU Kids Online Network

Loos M. / Helberger, N. / Guibault, L. / Mak, C. / Pessers, L. / Cseres, K. J. / van der Sloot, B. / Tigner, R. (2011), Final report Comparative analysis, Law & Economics analysis, assessment and development of recommendations for possible future rules on digital content contracts, available at: http://ec.europa.eu/justice/consumer-marketing/files/legal_report_final_30_august_2011.pdf

Loos, M. / Luzak, J. (2016), Wanted: A Bigger Stick, On Unfair Terms in Consumer Contracts with Online Service Providers, 39(1) Journal of Consumer Policy 63

Lupton, D. / Williamson, Ben. (2017), The datafied child: The dataveillance of children and implications for their rights, 19(5) New Media & Society 780

Mačėnaitė, M. (2017), From universal towards child-specific protection of the right to privacy online: dilemmas in the EU General Data Protection Regulation, 19(5) New Media and Society 765

Mačėnaitė, M. / Kosta E. (2017), Consent for processing children's personal data in the EU: following in US footsteps?, 26(2) Information & Communications Technology Law 146

Mak, V. (2010), Standards of Protection: In Search of the 'Average Consumer' of EU Law in the Proposal for a Consumer Rights Directive, TISCO Working Paper Series on Banking, Finance and Services No. 04/2010, June 2010

Mantelero, A. (2016), Children online and the future EU data protection framework: empirical evidences and legal analysis, 2(2–4) International Journal of Technology Policy and Law 169

Martin, M. C. (1997), Children's understanding of the intent of advertising: A meta-analysis, 16 Journal of Public Policy and Marketing 205

Mayer-Schönberger, V. / Cukier, K. (2013), The Rise of Big Data: How it's Changing the Way We Think about the World, 92 Foreign Affairs 28

McAnarney, E. R. (2008), Adolescent Brain Development: Forging New Links?, 42 Journal of Adolescent Health 321

McCreanor, T. / Barnes, H. M. / Gregory, M. / Kaiwai, H. / Borell, S. (2005), Consuming identities: Alcohol marketing and the commodification of youth experience, 13 Addiction Research & Theory 579

Mendoza, I. / Bygrave, L. A. (2017), The Right Not to Be Subject to Automated Decisions Based on Profiling, in: Synodinou, T. / Jougleux, P. / Markou, C. / Prastitou T. (Eds), EU Internet Law: Regulation and Enforcement, Springer

Micheti, A. / Burkell, J. / Steeves, V. (2010), Fixing Broken Doors: Strategies for Drafting Privacy Policies Young People Can Understand, Bulletin of Science, 30 Technology & Society 130

Micklitz, H. W. / Reisch, L. / Hagen, K. (2012), An Introduction to the Special Issue on "Behavioural Economics, Consumer Policy, and Consumer Law", 34 Journal of Consumer Policy 272

Montgomery, K. C. (2015), Youth and surveillance in the Facebook era: Policy interventions and social implications, 39 Telecommunications Policy 771

Montgomery, K. C. / Chester, J. (2015), Data protection for youth in the digital age: Developing a rights-based global framework, 1 European Data Protection Law Review 291

Noain-Sánchez, A. (2015), 'Privacy by default' and active 'informed consent' by layers: Essential measures to protect ICT users' privacy", 14(2) Journal of Information, Communication and Ethics in Society 124

Oates, C. / Blades, M. / Gunter, B. / Don, J. (2003), Children's understanding of television advertising: a qualitative approach, 9 Journal of Marketing Communications 59

Peter, J. / Valkenburg, P. (2011), Adolescents' online privacy: toward a developmental perspective, in: S. Trepte / L. Reinecke (Eds.), Privacy online, 221, Springer

Prenksy, M. (2001), Digital Natives, Digital Immigrants, 9 On the Horizon 1
Preston, C. B. / Crowther, B. T. (2014), Legal Osmosis: The Role of Brain Science in Protecting Adolescents, 43 (2) Hofstra Law Review 447
Rooney, T. / Taylor, E. (2017) (Eds.), Surveillance Futures: Social and Ethical Implications of New Technologies for Children and Young People, Routledge
Rozendaal, E. / Buijzen, M. / Valkenburg, P. (2010), Comparing Children's and Adults' Cognitive Advertising Competences in the Netherlands, 4 (1) Journal of Children and Media 77
Rozendaal, E. / Lapierre, M. A. / van Reijmersdal, E. A. / Buijzen, M. (2011), Reconsidering advertising literacy as a defense against advertising effects, 14 (4) Media Psychology, 338
Savin-Williams, R. C. / Berndt, T. J. (1990), Friendship and peer relations, in: S.S. Feldman & G. Elliot (Eds.), At the threshold: The developing adolescent, 277, Harvard University Press
Savirimuthu, J. (2016), Networked Children, Commercial Profiling and the EU Data Protection Reform Agenda: In the Child's Best Interests?, in: I. Iusmen / H. Stalford (Eds.), The EU as a Children's Rights Actor: Law, Policy and Structural Dimensions, 221, Barbara Budrich Publishers
Schaub, F. / Balebako, R. / Durity, A. L. / Cranor, L. F. (2015), A Design Space for Effective Privacy Notices, 11th Symposium on Usable Privacy and Security (SOUPS 2015), available at: https://www.usenix.org/system/files/conference/soups2015/soups15-paper-schaub.pdf
Sibony, A.-L. / Helleringer, G. (2015), EU Consumer Protection and Behavioral Sciences: Revolution or Reform?, in: A.-L. Sibony / A. Alemano (Eds.), Nudge and the Law: A European Perspective, 209, Hart Publishing
Steeves, V. (2014a), Young Canadians in a Wired World, Phase III: Online Privacy, Online Publicity, MediaSmarts
Steeves, V. (2014b), Young Canadians in a Wired World, Phase III: Life Online, MediaSmarts
Steeves, V. (2017), Terra Cognita: The Surveillance of Young Peoples' Favourite Websites, in: T. Rooney / E. Taylor (Eds.), Surveillance Futures: Social and Ethical Implications of New Technologies for Children and Young People, 174, Routledge
Steijn, W. M. P. (2014), Developing a sense of privacy, Phd dissertation, available at: https://pure.uvt.nl/ws/files/7737309/Steijn_Developing_05_09_2014_emb_tot_06_09_2015.pdf
Steijn, W. M. P. / Schouten, A. P. (2013), Information sharing and relationships on social network sites. 16 (8) Cyberpsychology, Behavior, & Social Networking 582
Steinberg, L. (2007), Risk taking in adolescence: New perspectives from brain and behavioral science, 16 Current Directions in Psychological Science 55
Steinberg, L. (2008), A social neuroscience perspective on adolescent risk-taking, 28 Developmental Review 78
Stuyck, J. / Terryn, E. / van Dyck, T. (2006), Confidence through fairness? The new directive on unfair business-to-consumer commercial practices in the internal market, 43 Common Market Law Review 107
Subrahmanyam, K. (2008), Communicating online: Adolescent relationships and the media, The Future of Children, 18 Children and Media Technology 119
Subrahmanyam, K. / Garcia, E. C. M. / Harsono, L. S. / Li, J. S. / Lipana, L. (2009), In their words: Connecting online weblogs to developmental processes, 27 British Journal of Developmental Psychology 219
Sunstein, C. R. (2014), Nudging: A Very Short Guide, 37 Journal of Consumer Policy 583
Svantesson, D. J. B. (2017), Enter the quagmire – the complicated relationship between data protection law and consumer protection law, Computer Law & Security Review, in press
Tapscott, D. (1998), Growing up digital: the rise of the Net generation, McGraw-Hill
Thaichon, P. (2017), Consumer socialization process: The role of age in children's online shopping behavior, 34 Journal of Retailing and Consumer Services 38
Third, A. / Bellerose, D. / Dawkins, U. / Keltie, E. / Pihl, K. (2014), Children's Rights in the Digital Age: A Download from Children Around the World, Young and Well Cooperative Research Centre

Valant, J. (2015), Consumer protection in the EU Policy overview, September 2015, available at: http://www.europarl.europa.eu/ReData/etudes/IDAN/2015/565904/EPRS_IDA(2015)565904_EN.pdf

Valkenburg, P. M. / Peter, J. (2008), Adolescents' identity experiments on the internet: consequences for social competence and self-concept unity, 35 (8) Communication Research 208

Van der Hof, S. (2016), I Agree, or Do I: A Rights-Based Analysis of the Law on Children's Consent in the Digital World, 34 Wis. Int'l L.J. 409

Van der Hof, S. / Prins C. (2008), Personalisation and its Influence on Identities, Behaviour and Social Values, in: Hildebrandt M. / Gutwirth S. (Eds.) Profiling the European Citizen: Cross–disciplinary perspectives, 111, Springer

Verdoodt, V. / Clifford, D. / Lievens, E. (2016), Toying with Children's Emotions, the New Game in Town? The Legality of Advergames in the EU, 32 Computer Law & Security Review 599

Waddington, L. (2014), Reflections on the Protection of 'Vulnerable' Consumers under EU Law, Maastricht Faculty of Law Working Paper No. 2013-2

Waterman, A. S. (1982), Identity development from adolescence to adulthood: an extension of theory and a review of research. 18 (3) Developmental Psychology 341

Wauters, E. / Lievens, E. / Valcke, P. (2013), A legal analysis of Terms of Use of Social Networking Sites, including a practical legal guide for users: 'Rights & obligations in a social media environment', EMSOC - User Empowerment in a Social Media Culture No. D1.2.4, iMinds-ICRI

Wauters, E. / Lievens, E. / Valcke, P. (2015), Children as social network actors: A European legal perspective on challenges concerning membership, rights, conduct and liability, 31 Computer Law & Security Review 351

Weitzenböck, E. M. (2014), Crowdsourcing and user empowerment: a contradiction in terms?, in: A. Savin / J. Trzaskowski (Eds.), Research Handbook on EU Internet Law, 461, Edward Elgar Publishing

Wong, R. / Savirimuthu, J. (2008), All or Nothing: this is the Question? The Application of Art. 3(2) Data Protection Directive 95/46/EC to the Internet, 25 (2) The John Marshall Journal of Information Technology and Privacy Law 241

Wu, H.-A. (2016), Video Game Prosumers: Case Study of a Minecraft Affinity Space, 42 Visual Arts Research 22

Xanthoulis, N. (2014), Negotiating the EU Data Protection Reform: Reflections on the Household Exemption, in: Sideridis A. / Kardasiadou Z. /Yialouris C. / Zorkadis V. (Eds.) E-Democracy, Security, Privacy and Trust in a Digital World, 135, Springer

Additional Sources

Article 29 Working Party, Opinion 10/2004 on more harmonised information provisions, WP 100, November 2004

Article 29 Data Protection Working Party, Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools), WP 160, 11 February 2009

Article 29 Data Protection Working Party, Opinion 5/2009 on Online Social Networking, WP 163, 12 June 2009

Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioral advertising, WP 171, 22 June 2010

Article 29 Data Protection Working Party, Opinion 02/2013 on Apps on Smart Devices, WP 202, 27 February 2013

Article 29 Data Protection Working Party, Statement of the Working Party on current discussions regarding the data protection reform package - Annex 2 Proposals for Amendments regarding exemption for personal or household activities, 27 February 2013

Consumer Protection Cooperation Network (2013), Common position of national authorities within the CPC on online games, available at: http://ec.europa.eu/consumers/enforcement/cross-border_enforcement_cooperation/docs/common_position_on_online_games_en.pdf

Consumer Protection Cooperation Network (2017), Common position of national authorities within the CPC Network concerning the protection of consumers on social networks, available at: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=55999

Belgian Privacy Commission (2002), Advice No. 38/2002 of 16 September 2002 concerning the protection of the private life of minors on the Internet, available at: https://www.privacycommission.be/sites/privacycommission/files/documents/advies_38_2002_0.pdf (Dutch); https://www.privacycommission.be/sites/privacycommission/files/documents/avis_38_2002_0.pdf (French)

EDPS (2012), Opinion on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – "European Strategy for a Better Internet for Children", 17 July 2012

EDPS (2014), Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, 14 March 2014

EDPS (2017), Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, 14 March 2017

Electronic Privacy Information Center (2012), In Short: Advertising and Privacy Disclosures in a Digital World, available at: https://epic.org/privacy/ftc/FTC-In-Short-Cmts-7-11-12-FINAL.pdf

European Commission (2017), Study on the application of the Consumer Rights Directive 2011/83/EU, Final report, May 2017, available at: https://ec.europa.eu/newsroom/document.cfm?doc_id=44637

European Commission (2017), Consumer Market Study to support the Fitness Check of EU consumer and marketing law, May 2017, available at: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=59332

European Commission (2016), Commission Staff Working Document, Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices, 25 May 2016, SWD(2016) 163 final

European Commission (2016), Consumer vulnerability across key markets in the European Union, Final report, January 2016, available at: http://ec.europa.eu/consumers/consumer_evidence/market_studies/docs/vulnerable_consumers_approved_27_01_2016_en.pdf

European Commission (2016), Study on the impact of marketing through social media, online games and mobile applications on children's behavior, March 2016, available at: http://ec.europa.eu/consumers/consumer_evidence/behavioural_research/docs/final_report_impact_marketing_children_final_version_approved_en.pdf

European Commission (2014), DG JUSTICE Guidance Document concerning Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, 13 June 2014, available at: http://ec.europa.eu/justice/consumer-marketing/files/crd_guidance_en.pdf

European Commission (2014b), Commission and Member States to raise consumer concerns with app industry, Press Release, 27 February 2014, available at: http://europa.eu/rapid/press-release_IP-14-187_en.htm

European Consumer Consultative Group (2013), Opinion on Consumers and Vulnerability, 7 February 2013, available at: http://ec.europa.eu/consumers/empowerment/docs/eccg_opinion_consumers_vulnerability_022013_en.pdf

European Parliament (2012), Report on a strategy for strengthening the rights of vulnerable consumers, 8 May 2012 (2011/2272(INI)), available at: http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2012-0155&language=EN

European Parliament (2014), Legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 –2012/0011(COD)), P7_TA(2014)0212

Eurostat (2016) E-commerce statistics for individuals, available at: http://ec.europa.eu/eurostat/statistics-explained/index.php/E-commerce_statistics_for_individuals#Proportion_of_e-shoppers_growing_steadily.2C_with_the_biggest_increase_among_young_people

Finnish competition and Consumer Authority (2015), Facts and Advice: A child needs a parent's consent to make purchases, available at: http://www.kkv.fi/en/facts-and-advice/buying-and-selling/children-as-consumers/children-as-shoppers/

Forbrukerrådet (the Norwegian Consumer Council) (2016), #Toyfail: An analysis of consumer and privacy issues in three internet-connected toys, available at: https://fil.forbrukerradet.no/wp-content/uploads/2016/12/toyfail-report-desember2016.pdf

ICO (2016), The Guide to Data Protection, 11 May 2016, available at: https://ico.org.uk/media/for-organisations/guide-to-data-protection-2-4.pdf

International Conference of Data Protection and Privacy Commissioners (2009), International Standards on the Protection of Privacy with regard to the processing of Personal Data (the Madrid Resolution), 5 November 2009

OFCOM (2016), Children and parents: media use and attitudes report, available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0034/93976/Children-Parents-Media-Use-Attitudes-Report-2016.pdf

Office of Fair Trading (2014), The OFT's Principles for online and app-based games, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/288360/oft1519.pdf

The Guardian, Facebook told advertisers it can identify teens feeling 'insecure' and 'worthless', 1 May 2017

UK Advertising Standard Authority (2010), UK Code of Non-broadcast Advertising, Sales Promotion and Direct Marketing, edition 12

UK Children's Commissioner (2017), Growing up Digital: A Report of the Growing Up Digital Taskforce, available at: https://www.childrenscommissioner.gov.uk/wp-content/uploads/2017/06/Growing-Up-Digital-Taskforce-Report-January-2017_0.pdf

UN Committee on the Rights of the Child, General Comment No. 12: The Right of the Child to be Heard, UN Doc. CRC/C/GC/12, 20 July 2009

Personal-Data and Consumer Protection: What Do They Have in Common?

Matilde Ratti

Contents

1 Premises 378
2 A Weaker Subject to be Protected 378
3 Similar Regulatory Techniques for Data-Subject and Consumer Protection 379
4 Information Requirements for Contracts and Data Processing 381
5 Withdrawal from the Contract and Withdrawal of Consent: The Same Rationale? 385
6 Jurisdiction Rules: An International Scenario 386
7 Data Processing and B2C Contracting in the Global Market 388
8 Two Emerging Critical Issues to be Settled 390
References 391

Abstract The European legislature deals with personal-data and consumer protection with two approaches which have a lot in common. Both the European law on the processing of personal data and that on B2C contracts focus on the protection of a weaker subject and they seem to be based on similar legal instruments: the information requirements, the recognition of specific rights to consumers and data subjects (in particular, the right to withdraw) and the provision of favourable litigation rules for the weaker party. This paper analyses the similarities existing between regulatory techniques adopted by the present legislation in order to determine the level of protection granted and whether a holistic approach to the subject is possible or desirable.

Matilde Ratti, PhD in Civil Law, is a Research Fellow and Adjunct Professor at the University of Bologna Alma Mater Studiorum, Department of Private Law.

M. Ratti (✉)
Department of Private Law, University of Bologna, Bologna, Italy
e-mail: matilde.ratti@unibo.it

M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law*, MPI Studies on Intellectual Property and Competition Law 28, https://doi.org/10.1007/978-3-662-57646-5_14

1 Premises

European consumer and personal-data-protection rules provide a solution to similar juridical issues, since both aim to grant a minimum level of protection to physical persons acting on the market, the consumer[1] and the data subject.[2] In electronic commerce, these two subjects act in very similar situations: they interact on the computer, rather than in a physical space, they stipulate contracts with a counterpart who has more information than they do and who deals with a multitude of subjects online.[3] Furthermore, in most of the juridical relationships, the consumer and the data subject are indeed the same person.

In such a scenario, it seems useful to consider and to analyse the laws on consumer and personal-data protection with a holistic approach, in order to determine whether any similarity exists between the two disciplines, whether the present legislation provides effective protection, whether the adoption of different or additional legal techniques could be advisable and whether a holistic approach is desirable.

2 A Weaker Subject to be Protected

In attempting to analyse the existing relationship between the European legislation on personal-data and consumer protection, Directive 2011/83/EU on consumer rights,[4] Directive 95/46/EC on the processing of personal data[5] and the recently

[1] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011, on consumer rights, published in the Official Journal of the European Union L 304/64, 22 November 2011, Article 2(1) states that 'consumer' 'means any natural person who, in contracts covered by this Directive, is acting for purposes which are outside his trade, business, craft or profession'.

[2] The data subject is referred to in Article 2 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Union L 281, 23 November 1995. Article 2(a)), of Directive 95/46/EC establishes that personal data mean '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'.

[3] For an analysis of the juridical issues connected to the use of electronic communications for the conclusion of contracts see Finocchiaro (2014), 605; Finocchiaro / Delfini (2014); Smedinghoff (1999), 140 and Smedinghoff (1996); Finocchiaro (1997); Gambino (1997); Edwards / Weald (1997); Caprioli / Sorieul (1997), 323; Smedinghoff (1996).

[4] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, published in the Official Journal of the European Union L 304/64, 22 November 2011. On the Directive, see Luzak (2015); Luzak / Mak (2013). For an analysis of the Directive in the context of European consumer contract law, see Halls / Howells / Watson (2012), 151; Micklitz (2012), 6; Hesselink (2007), 323. In the Italian scenario, see Falce (2011), 327.

[5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement

adopted General Data Protection Regulation 2016/679/EU (GDPR)[6] should all be taken into consideration.

First of all, it seems relevant to highlight that these three pieces of law aim to protect the weaker subject. In fact, data subjects and consumers are considered, and in most cases they are, much weaker than their counterparts, i.e. data controllers and traders. As it is well known, the trader acts for trade, business, craft or professional purposes in relation to B2C contracts.[7] In fact, traders can rely on their professional experience, while consumers only act for personal purposes. Similarly, data subjects are often unaware of being in charge of their data and have no idea of being profiled or of their data being processed by a data controller.[8]

3 Similar Regulatory Techniques for Data-Subject and Consumer Protection

From a general point of view, European laws on the processing of personal data and on B2C contracts aim at providing transparency, granting rights to the weaker party and imposing obligations on traders and data controllers.

To be precise, the Consumer Rights Directive establishes that a trader is obliged to accurately inform data subjects of the contract terms and the goods exchanged.[9] Articles 9 to 16 of Directive 2011/83/EU are dedicated to the right of withdrawal, to the consequences for failing to provide all necessary information on such a right and to the parties' obligations in case of withdrawal from a contract.[10] Furthermore, in

---

of such data, published in the Official Journal of the European Union L 281, 23 November 1995. For an analysis of the application of Directive 95/46/EC in the Italian scenario, see Finocchiaro (2012) and, for an Italian perspective on European privacy law, see Macario (1997).

[6] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, published in the Official Journal of the European Union L 119/1, 4 May 2016. For an analysis of the GDPR see Twigg-Flesner (2012). In the Italian scenario, see Finocchiaro (2017).

[7] Article 2, No. 2, of the Consumer Rights Directive defines the 'trader' as 'any natural person or any legal person, irrespective of whether privately or publicly owned, who is acting, including through any other person acting in his name or on his behalf, for purposes relating to his trade, business, craft or profession in relation to contracts covered by this Directive'.

[8] Article 4, No. 7, of the GDPR defines the 'controller' as 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data'.

[9] Furthermore, when the contract is concluded online, Articles 6 and 8 of the Directive impose specific additional form and information requirements.

[10] Chapter IV of Directive 2011/83/EU establishes further consumer rights: Article 18 states rules on the timing of the delivery of goods, Article 20 imposes the risk of loss of or damage to the goods on the trader until the consumer has physical possession of the goods, Article 21 establishes a rate limit for consumers' telephone calls related to B2C contracts and Article 22 recognises consumer rights to be informed in advance of any additional cost.

case of litigation, the European Regulation 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters[11] establishes specific rules over consumer contracts. Therefore, it seems possible to identify at least three different legal instruments provided for by the European legislation on B2C contracts aiming to grant consumer protection: the information requirements to be met by the trader, the consumer right to withdraw (among other rights) and the jurisdictional protection.

A similar regulatory technique seems to be in place for the protection of personal data. The processing of personal data is currently governed (and will be just until May 2018) by Directive 95/46/EC, which states the general principles for the lawful processing of personal data. Data controllers must ask data subjects' consent for processing their data.[12] Like the Consumer Rights Directive, Directive 95/46/EC establishes the information that data controllers must provide when collecting data (Articles 10 and 11) and recognises other rights of data subjects: the right to access personal data (Article 12), the right to object to the processing and the right to withdraw their consent (Article 14). Furthermore, the GDPR, which will soon repeal Directive 95/46/EC, has adopted the same approach. Personal-data processing is based on informed consent, specific rights, such as the right to withdraw, are recognised for data subjects[13] and the data subjects' right to an effective judicial remedy against the controller is established.[14]

This overview seems to confirm that both the European law on consumer protection and the European law on the protection of personal data have adopted at least three similar legal instruments to protect consumers and data subjects. In fact, both the GDPR and the Consumer Rights Directive impose information requirements on the controller and on the trader, recognise specific rights for the weaker subjects (in particular the right to withdraw) and provide them with favourable litigation rules.

[11] Regulation 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, published in the Official Journal of the European Union L 351/1, 20 December 2012, in Section IV establishes specific rules on B2C contracts.

[12] Moreover, Article 7 of Directive 95/46/EC states that personal data may be legitimately processed even without consent in certain circumstances. For instance, the data controller might process personal data if this is necessary for the performance of a contract or to comply with legal obligations.

[13] Articles 12 to 14 of the GDPR establish the right to transparent information and specify what information data controllers must provide when collecting data. Articles 15 and 16 establish data subjects' right to access their personal data and to rectify them. Furthermore, the GDPR introduces some new rights, such as the right to be forgotten (Article 17) and the right to data portability (Article 20).

[14] See Chapter VIII of the GDPR on Jurisdiction Rules.

4 Information Requirements for Contracts and Data Processing

In order to verify to what extent the similarities between the juridical techniques mentioned above exist and to determine whether such techniques are equally effective in granting protection to weaker subjects, they will be analysed one by one.

Regarding the information requirements, according to the GDPR and to the Consumer Rights Directive, both data controllers and traders have to provide all necessary information before processing personal data and before concluding the contract.

Data controllers should provide the data subject with the information enumerated in Articles 13 and 14 of the GDPR.[15] To be precise, Article 13 refers to the case of the personal data collected from the data subject, while Article 14 applies when personal data have not been collected or obtained from the data subject. In this case, the controller must provide the information within a reasonable period of time after obtaining the personal data. The reasonable period of time can be determined having regard to the specific circumstances in which the personal data is processed, but the information should be provided no later than one month after obtainment.[16] Thus, the general rule consists of providing data subjects with all necessary information when the personal data is directly collected from them. In case personal data is collected from a different source, the controller should provide the information within a reasonable period of time. For example, in the case of the conclusion of a contract between two parties, the data subject, who is possibly a consumer as well, should receive all necessary information at the time he or she provides his or her personal data to the other party.[17]

According to both Articles 13 and 14 of the GDPR, all data subjects should receive accurate information about the identity and the contact details of the controller and of the data protection officer. Data subjects should also be informed about the purposes of the processing, the legal basis for the processing and the recipients or categories of recipients of the personal data. If the data controller intends to transfer personal data to a third country or international organisation, data subjects should be informed.[18] Among the information listed in Articles 13 and 14

[15] See Articles 10 and 11 of Directive 95/46/EC on the processing of personal data.

[16] Article 14(3) also provides that if personal data is to be used for communication with the data subject, the controller must provide the information at the latest at the time of the first communication to the data subject or, if a disclosure to another recipient is envisaged, at the latest when the personal data is first disclosed.

[17] Article 14(5) establishes that data controllers are not obliged to provide information when this involves a disproportionate effort, in particular if the processing serves archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In such cases the controller must take appropriate measures to protect the data subject's rights and legitimate interests, including making the information publicly available.

[18] They should also be made aware of the existence or absence of an adequacy decision made by the Commission. If the processing is necessary for legitimate interests of the controller, data subjects

of the GDPR, the controllers' obligation to indicate the storage period of the data[19] and the existence of the right of access, rectification or erasure is also worth mentioning. The data controller should also mention the existence of the data subject's right to object to the processing, to data portability, to withdraw the consent and to lodge a complaint with a supervisory authority. Furthermore data subjects should be informed on whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as on whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.

Like the GDPR, the Consumer Rights Directive establishes the traders' obligation to provide consumers with information.[20] More specifically, in the case of distance contracts,[21] the information requirements should be adapted to any existing technical constraint. In such cases, the trader should comply with a minimum set of information requirements and refer the consumer to another source of information, for instance by providing a hypertext link to a webpage of the trader where the relevant information is directly available. To this effect, regarding distance contracts, Article 8 of the Consumer Rights Directive specifically establishes that the trader must give all necessary information 'in a way appropriate to the means of distance communication used in plain and intelligible language'.[22] Such information should

should be informed about the legitimate interests pursued by the controller or by a third party as well. For cases in which personal data has not been obtained from the data subject, Article 14 of the GDPR also provides that the data subjects should be informed of the categories of personal data concerned by the processing (Article 14(1)(d)), of the source of the personal data and on whether data came from publicly accessible sources (Article 14(2)(f)).

[19] The period for which the personal data will be stored or, if that is not possible, the criteria used to determine that period.

[20] The information should be given in a clear and comprehensible way, so as to protect the consumer who is in a weaker position by lending transparency to the contract. The information to be provided by the trader to the consumer is mandatory and may not be altered.

[21] According to Article 2(7) of Directive 2011/83/EU, 'distance contract' 'means any contract concluded between the trader and the consumer under an organised distance sales or service-provision scheme without the simultaneous physical presence of the trader and the consumer, with the exclusive use of one or more means of distance communication up to and including the time at which the contract is concluded'. On the definition of 'distance contract', the European Commission, Commission Staff Working Document, Accompanying Document to the Proposal for a Consumer Rights Directive, Annexe, specifies that the current definition of distance contract has led to different interpretations in Member States. The Commission observes: 'there are different views if the whole or only parts of the sales process have to take place through means of distance communication for the contract to be considered a distance contract. [F]urthermore, uncertainties arise as to whether contracts negotiated away from business premises, but concluded by means of distance communication should be considered to be distance selling or off-premises sales'.

[22] Both Chapter II, Consumer information for contracts other than distance or off-premises contracts, and Chapter III, Consumer information and right of withdrawal for distance and off-premises contracts, of Directive 2011/83/EU establish an information requirement for the respective types of contracts. For a complete analysis of the information requirements, see Mankowski (2005), 779.

be provided before the consumer is bound by the contract. Article 6 of the Consumer Rights Directive lists the necessary information to be provided.[23] For instance, the

[23] Article 6 of the Consumer Rights Directive establishes that:

1. Before the consumer is bound by a distance or off-premises contract, or any corresponding offer, the trader shall provide the consumer with the following information in a clear and comprehensible manner:

(a) the main characteristics of the goods or services, to the extent appropriate to the medium and to the goods or services;

(b) the identity of the trader, such as his trading name;

(c) the geographical address at which the trader is established and the trader's telephone number, fax number and e-mail address, where available, to enable the consumer to contact the trader quickly and communicate with him efficiently and, where applicable, the geographical address and identity of the trader on whose behalf he is acting;

(d) if different from the address provided in accordance with point (c), the geographical address of the place of business of the trader, and, where applicable, that of the trader on whose behalf he is acting, where the consumer can address any complaints;

(e) the total price of the goods or services inclusive of taxes, or where the nature of the goods or services is such that the price cannot reasonably be calculated in advance, the manner in which the price is to be calculated, as well as, where applicable, all additional freight, delivery or postal charges and any other costs or, where those charges cannot reasonably be calculated in advance, the fact that such additional charges may be payable. In the case of a contract of indeterminate duration or a contract containing a subscription, the total price shall include the total costs per billing period. Where such contracts are charged at a fixed rate, the total price shall also mean the total monthly costs. Where the total costs cannot be reasonably calculated in advance, the manner in which the price is to be calculated shall be provided;

(f) the cost of using the means of distance communication for the conclusion of the contract where that cost is calculated other than at the basic rate;

(g) the arrangements for payment, delivery, performance, the time by which the trader undertakes to deliver the goods or to perform the services and, where applicable, the trader's complaint handling policy;

(h) where a right of withdrawal exists, the conditions, time limit and procedures for exercising that right in accordance with Article 11(1), as well as the model withdrawal form set out in Annex I(B);

(i) where applicable, that the consumer will have to bear the cost of returning the goods in case of withdrawal and, for distance contracts, if the goods, by their nature, cannot normally be returned by post, the cost of returning the goods;

(j) that, if the consumer exercises the right of withdrawal after having made a request in accordance with Article 7(3) or Article 8(8), the consumer shall be liable to pay the trader reasonable costs in accordance with Article 14(3);

(k) where a right of withdrawal is not provided for in accordance with Article 16, the information that the consumer will not benefit from a right of withdrawal or, where applicable, the circumstances under which the consumer loses his right of withdrawal;

(l) a reminder of the existence of a legal guarantee of conformity for goods;

(m) where applicable, the existence and the conditions of after sale customer assistance, after-sales services and commercial guarantees;

(n) the existence of relevant codes of conduct, as defined in point (f) of Article 2 of Directive 2005/29/EC, and how copies of them can be obtained, where applicable;

(o) the duration of the contract, where applicable, or, if the contract is of indeterminate duration or is to be extended automatically, the conditions for terminating the contract;

(p) where applicable, the minimum duration of the consumer's obligations under the contract;

trader must provide information about the characteristics of the goods and services, and about the identity of the trader and its geographical address. The total price of the goods or services, inclusive of taxes, should be clearly expressed with all additional freight, delivery or postal charges. The arrangements for payment, delivery, performance, the time by which the trader undertakes to deliver the goods or to perform the services are also to be indicated. Like the GDPR, Article 6(1)(h) of the Consumer Rights Directive obliges the trader to inform the consumer about the existence of a right to withdraw from the contract and about the conditions, time limit and procedures for exercising that right. Furthermore, the trader should also add a reminder of the existence of a legal guarantee of conformity for goods and the duration of the contract. If the contract is of indeterminate duration or is to be extended automatically, the conditions for terminating the contract should also be indicated.

(q) where applicable, the existence and the conditions of deposits or other financial guarantees to be paid or provided by the consumer at the request of the trader;

(r) where applicable, the functionality, including applicable technical protection measures, of digital content;

(s) where applicable, any relevant interoperability of digital content with hardware and software that the trader is aware of or can reasonably be expected to have been aware of;

(t) where applicable, the possibility of having recourse to an out-of-court complaint and redress mechanism, to which the trader is subject, and the methods for having access to it.

2. Paragraph 1 shall also apply to contracts for the supply of water, gas or electricity, where they are not put up for sale in a limited volume or set quantity, of district heating or of digital content which is not supplied on a tangible medium.

3. In the case of a public auction, the information referred to in points (b), (c) and (d) of paragraph 1 may be replaced by the equivalent details for the auctioneer.

4. The information referred to in points (h), (i) and (j) of paragraph 1 may be provided by means of the model instructions on withdrawal set out in Annex I (A). The trader shall have fulfilled the information requirements laid down in points (h), (i) and (j) of paragraph 1 if he has supplied these instructions to the consumer, correctly filled in.

5. The information referred to in paragraph 1 shall form an integral part of the distance or off-premises contract and shall not be altered unless the contracting parties expressly agree otherwise.

6. If the trader has not complied with the information requirements on additional charges or other costs as referred to in point (e) of paragraph 1, or on the costs of returning the goods as referred to in point (i) of paragraph 1, the consumer shall not bear those charges or costs.

7. Member States may maintain or introduce in their national law language requirements regarding the contractual information, so as to ensure that such information is easily understood by the consumer.

8. The information requirements laid down in this Directive are in addition to information requirements contained in Directive 2006/123/EC and Directive 2000/31/EC and do not prevent Member States from imposing additional information requirements in accordance with those Directives.

Without prejudice to the first subparagraph, if a provision of Directive 2006/123/EC or Directive 2000/31/EC on the content and the manner in which the information is to be provided conflicts with a provision of this Directive, the provision of this Directive shall prevail.

9. As regards compliance with the information requirements laid down in this Chapter, the burden of proof shall be on the trader.

Both the GDPR and the Consumer Rights Directive prescribe information requirements to be met before (when this is possible) the conclusion of the contract and before the processing of personal data. Nevertheless, doubts can arise regarding the effectiveness of such a legal technique, since in both cases consumers and data subjects often do not read the information provided.[24]

5 Withdrawal from the Contract and Withdrawal of Consent: The Same Rationale?

Similar considerations can be made on the right to withdraw provided for by the General Data Protection Regulation and by the Consumer Rights Directive. The consumer is indeed granted a period of 14 days to withdraw from a distance or off-premises contract by Article 9 of the Consumer Rights Directive and, according to Article 14 of the GDPR, data subjects can withdraw their consent to the processing of personal data anytime. Neither the consumer nor the data subject is required to justify the withdrawal.

Therefore, the right of withdrawal seems to be the second juridical instrument chosen by the European legislature to safeguard the weaker subject's position. Nevertheless, from a systematic point of view, it should be considered that the juridical relationships existing between traders and consumers and between controllers and data subjects are different. In fact, after the fourteenth day from the conclusion of the contract (for service contracts) or from the day of the acquisition of physical possession of the goods (for sales contracts)[25] consumers are party to a binding contract concluded with the trader. Data subjects, on the other hand, can always withdraw their consent to the processing of personal data. Such a difference is related to the nature of the right protected in the two situations. In fact, consumers

[24] When a lot of information is provided, it is possible (or even likely) that people will not read it, or will not understand it, if they have read it. With regard to privacy policies, this has been highlighted by Turow / Feldman / Meltzer (2005) and Cranor / Reidenberg (2002).

[25] For sales contracts, when the consumer orders multiple goods in one order, but they are delivered separately, the 14-day period starts on the day on which the consumer (or a third party other than the carrier indicated by the consumer) acquires physical possession of the last good. Similarly, in the case of delivery of a good consisting of multiple lots, the 14-day period starts on the day on which the consumer acquires physical possession of the last lot. In the case of contracts for regular delivery of goods, the withdrawal period starts from the day on which the consumer acquires physical possession of the first good. In the case of contracts for the supply of water, gas or electricity, where they are not put up for sale in a limited volume or set quantity, the 14-day period starts on the day of the conclusion of the contract. For further specification on the calculation of the right-of-withdrawal period, see European Commission, DG Justice, DG Justice Guidance Document Concerning Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and June 2014 of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, June 2014, 37.

take part in a binding contract, while data subjects' right to protection of personal data falls under the definition of fundamental rights.

Personal-data protection is indeed recognised by Article 8 of the Charter of Fundamental Rights of the European Union.[26] Personal data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Such a right has been classified as fundamental and, as such, cannot become the subject of any contract. For such a reason, the data subject withdrawal right provided for by the GDPR has no time limit.

6 Jurisdiction Rules: An International Scenario

Another relevant similarity between the European legislation on consumer and personal-data protection emerges in relation to the protection of the weaker subject in the pathological phase of the relationship. In fact, in case of litigation, both the European Regulation 1215/2012 on jurisdiction and recognition and enforcement of judgments in civil and commercial matters[27] and the GDPR favour the place of residence or domicile of the weaker party to the juridical relationship.

The Jurisdiction Regulation establishes the applicable jurisdiction rules over consumer contracts in Section IV, from Article 17 to Article 19. To be precise, Article 18 of the Jurisdiction Regulation establishes that consumers may bring proceedings against the other party to a contract either in the courts of the Member State in which that party is domiciled[28] or in the courts of the place where the

[26] Charter of Fundamental Rights of the European Union, published in the Official Journal of the European Union (Communities), 2000/C 364/01, 18 December 2000. Article 8 establishes: '1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority'.

For an analysis of the legal value of the Charter, see Lord Goldsmith (2001), 1204 and Eeckhout (2001), 947. For a study on human rights in Europe after the Treaty of Lisbon, see Douglas-Scott (2011), 645, who underlines that already in the first two years after the entry into force of the Lisbon Treaty, the Charter had been referred to on many occasions by the European Court of Justice and that it now operates as the primary source of human rights in the EU. In the Italian scenario, see Manzella / Melograni / Paciotti / Rodotà (2001).

[27] Regulation 1215/2012 of the European Parliament and of the Council, of 12 December 2012, on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, published in the Official Journal of the European Union L 351/1, 20 December 2012.

[28] It should also be noted that, according to Article 17(2) of the Jurisdiction Regulation, the trader whose branch, agency or other establishments is in one of the Member States, is considered to be domiciled in the Member State in relation to the disputes arising out of the branch, agency or establishment of the trader. Article 17(2) of the Jurisdiction Regulation specifically states that 'where a consumer enters into a contract with a party who is not domiciled in a Member State but has a branch, agency or other establishment in one of the Member States, that party shall, in

consumer is domiciled. In other words, consumers can choose to bring proceedings before their court or the trader's court, regardless of the domicile of the other party. Furthermore, the provision also ensures to consumers the right not to be brought before any other court than the one of their domicile (Article 18(2)).[29]

The provisions just illustrated can be derogated by the parties to a B2C contract, but only after the dispute has arisen and with a subsequent agreement which allows the consumer to bring proceedings in courts other than those indicated by Article 18 of the Jurisdiction Regulation. If such an agreement is made between parties domiciled or habitually resident in the same Member State at the time of conclusion of the contract, the agreement should establish the jurisdiction of the courts of that Member State.

Therefore, the rules established in relation to the jurisdiction on B2C contracts allow consumers to choose the court before which to raise their complaints and protects them from the choice of a less favourable jurisdiction by traders.

It seems that similar rights are recognised by the GDPR to the data subject. Indeed, Article 79(2) of the GDPR states that proceedings against a controller or a processor must be brought before the courts of the Member State where the controller or the processor has an establishment.[30] Otherwise, proceedings may be

---

disputes arising out of the operations of the branch, agency or establishment, be deemed to be domiciled in that Member State'.

[29] Article 18 of the Jurisdiction Regulation establishes that '1. A consumer may bring proceedings against the other party to a contract either in the courts of the Member State in which that party is domiciled or, regardless of the domicile of the other party, in the courts for the place where the consumer is domiciled.

2. Proceedings may be brought against a consumer by the other party to the contract only in the courts of the Member State in which the consumer is domiciled.

3. This Article shall not affect the right to bring a counterclaim in the court in which, in accordance with this Section, the original claim is pending'.

It should be underlined that, according to Article 17 of the Jurisdiction Regulation, rules established by Article 18 only apply if the contract has been concluded with a trader who pursues commercial or professional activities in the Member State of the consumer's domicile or, if the trader directs the activities to that Member State (or to several States including that Member State) and the contract falls within the scope of such activities. Article 18 also applies to contracts for the sale of goods on instalment credit terms, to contracts for a loan repayable by instalments or for any other form of credit made to finance the sale of goods. This rule does not apply, however, to contracts of transport other than a contract which, for an inclusive price, provides for a combination of travel and accommodation.

[30] The notion of establishment has been variously interpreted through the years. In the field of personal data protection, such a notion is also crucial in determining the applicability of Directive 95/46/EC to personal data processing, since Article 4(1), of Directive 95/46/EC establishes that '1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

Some differences can be highlighted between the jurisdiction rules applicable to disputes arising from B2C contracts or from the processing of personal data. While consumers can bring proceedings before the courts of the Member State of their domicile, the GDPR refers to the data subject's habitual residence. Furthermore, if the data controller or processor is a public authority processing personal data in the exercise of its public powers, data subjects' right to bring the proceeding before the courts of the Member State of their habitual residence is limited. Such a limitation seems designed to avoid rulings by national judges on matters affecting another Member State's public authorities. However, both consumers and data subjects have the right to choose to bring the proceeding before the courts of the Member States in which they have their habitual residence or domicile.

7 Data Processing and B2C Contracting in the Global Market

The provisions on jurisdiction have been set in a context in which data is exchanged and contracts are concluded online, even among parties located in different countries. In such a scenario, it also seems appropriate to examine and compare the European drafting techniques on the applicable law. According to Regulation 593/2008 on the law applicable to contractual obligations[31] (Rome I Regulation) contracts concluded with consumers are subject to the law of the country in which

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community'.

On the applicability of Directive 95/46/EC see Kuner (2007); Moerel (2011), 92; Colonna (2014), 203. Lately, the ECJ, in Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, C. 230/14, ECLI:EU:C:2015:639 expressed the need of an extensive interpretation of the notion of establishment. At paras. 29, 30 and 31 of the Weltimmo decision, the Court states that 'as the Advocate General observed, in essence, in points 28 and 32 to 34 of his Opinion, this results in a flexible definition of the concept of 'establishment', which departs from a formalistic approach whereby undertakings are established solely in the place where they are registered. Accordingly, in order to establish whether a company, the data controller, has an establishment, within the meaning of Directive 95/46, in a Member State other than the Member State or third country where it is registered, both the degree of stability of the arrangements and the effective exercise of activities in that other Member State must be interpreted in the light of the specific nature of the economic activities and the provision of services concerned. […]. It should be considered that the concept of 'establishment', within the meaning of Directive 95/46, extends to any real and effective activity - even a minimal one - exercised through stable arrangements'.

[31] Regulation 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), published in the Official Journal of the European Union L 177/6, 4 July 2008.

they have their habitual residence.[32] In order for this rule to apply, the contract must fall within the scope of the trader's professional activities and such activities must be carried out in the country where the consumer has his or her habitual residence or must at least be directed to that country, or to several countries including that one.[33]

Parties are also allowed to choose the law applicable to the contract, but this choice may not deprive consumers of the protection that would be afforded by the law which would have been applicable if the parties had not made any choice. With such a provision, the Rome I Regulation establishes a minimum level of protection for consumers regardless of any choice of applicable law.

Article 6 of the Rome I Regulation seems to adopt the same logic as Article 3 of the GDPR. In fact, the GDPR is applicable if the data processing is carried out by a controller in the European Union or, for certain services, even if the controller is not established in Europe, but the data subject is.[34]

According to its Article 3 the GDPR applies to the processing of personal data by the establishment of a controller or a processor in the European Union, regardless of whether the processing takes place in the Union or not. Furthermore, if data subjects are in the European Union, the Regulation applies even to controllers or processors

[32] Article 6(1) of Regulation 593/2008: 'Without prejudice to Articles 5 and 7, a contract concluded by a natural person for a purpose which can be regarded as being outside his trade or profession (the consumer) with another person acting in the exercise of his trade or profession (the professional) shall be governed by the law of the country where the consumer has his habitual residence, provided that the professional:

(a) pursues his commercial or professional activities in the country where the consumer has his habitual residence, or

(b) by any means, directs such activities to that country or to several countries including that country, and the contract falls within the scope of such activities'.

[33] According to Article 6(4) of the Rome I Regulation, some contracts are not subjects to the rules established in the Article, such as contracts for the supply of services where the services are to be supplied to consumers exclusively in a country other than the one where they have their habitual residence, contracts of carriage other than a contract relating to package travel within the meaning of Council Directive 90/314/EEC of 13 June 1990 on package travel, package holidays and package tours, contracts relating to a right in rem in immovable property or a tenancy of immovable property other than a contract relating to the right to use immovable properties on a timeshare basis within the meaning of Directive 94/47/EC.

[34] On this matter, the GDPR adopts a different approach than Directive 95/46/EC. Directive 95/46/EC currently provides for the applicability of the Member States' law if the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State. The adoption of the principle of the applicability of European law to the data subject within the European territory by the GDPR seems to have been influenced by some of the EU Court of Justice Decisions, e. g. ECJ, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, C-131/12, ECLI:EU:C:2014:317 and ECJ, Maximillian Schrems v Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650. On the case Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, see also Article 29 Data Protection Working Party, Guidelines on the Implementation of ECJ, Google Spain And Inc V. Agencia Española De Protección De Datos (Aepd) And Mario Costeja González, C-131/12, ECLI:EU:C:2014:317, adopted on 26 November 2014 (14/EN WP 225). For a juridical analysis of the two decisions, see Finocchiaro (2015), 787.

who are not established in Europe if the data processing is related to the offering of goods or services to data subjects in the Union or to the monitoring of their behaviour in the Union.[35]

Therefore, the European GDPR and the Consumer Rights Directive are applicable to disputes connected to data subjects or consumers who are, or whose habitual residence is, in Europe.

8 Two Emerging Critical Issues to be Settled

Examining consumer and personal-data-protection laws with a holistic perspective is essential to reveal consumers' and data subjects' weaker position and to highlight the many analogies existing between the two disciplines. The analysis carried out has demonstrated that both the European laws on consumer rights and on personal-data protection adopt the same instruments in order to protect the weaker subject.

They establish information requirements to be met by traders and data controllers before the juridical relationship with the consumer and with the data subjects begins, or, if this is not possible, within a limited period of time. However, as concerns the effectiveness of such a measure, one could observe that consumers and data subjects often do not read the information provided.

Both the disciplines provide for the right to withdraw, as consumers can withdraw from B2C contracts and data subjects can, in principle, decide not to allow the processing of their personal data anytime. However, if the processing is necessary for the performance of the contract or according to legal provisions or to other circumstances provided for by the GDPR, the right to withdraw from contracts is just applicable in theory.

Finally, it has been observed that both data subjects and consumers are granted jurisdiction rules which allow them to bring proceedings before the courts of the Member States where they have their habitual residence or domicile.

The analysis presented here on the regulatory techniques in European consumer and data-protection law has outlined two main issues to be settled. While the European legislation in both areas in fact adopts the same legal approach to protect weaker subjects, it should not be forgotten that the Consumer Rights Directive aims to balance the contractual interests of two parties to a contract, while the GDPR and Directive 95/46/EC on the processing of personal data protect a fundamental right. Providing the same legal instruments to deal with these two different situations may

[35] Article 3 of the GDPR also provides for the case of conflict of law resulting in the applicability of a law of one of the European Member States. To this end, Article 3(3) establishes that the Regulation applies 'to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law'.

lead to the possibly critical conclusion that a fundamental right could be dealt with by a contractual approach.[36]

The effectiveness of the protection provided by the legal instruments examined is the second emerging issue.[37] The European legislature's approach is a formalistic one and seems not to offer a significant protection to the weaker party, since data subjects and consumers rarely read the information provided and are barely aware of their right of withdrawal.

References

Caprioli, E.A. / Sorieul, R. (1997), Le commerce international électronique: vers l'émergence de règles juridiques transnationales, 124 Journal du droit international, 323

Cate, F. H. (2006), The Failure of Fair Information Practice Principles, in: J. K. Winn (Ed.), Consumer Protection in the Age of the 'nformation Economy', Ashgate Publishing

Colonna, L. (2014), Article 4 of EU Data Protection and the Irrelevance of the EU-US Safe Harbor Program? International Data Privacy Law, 203

Cranor, L. F. / Reidenberg, J. (2002), Can User Agents Accurately Represent Privacy Notices?, The 30th Research Conference on Communication, Information, and Internet Policy, Alexandria, Virginia

Douglas-Scott, S. (2011), The European Union and Human Rights after the Treaty of Lisbon, Human Rights Law Review, 11:4, 645

Edwards, L. / Weald, C. (1997), Law and the Internet: Regulating Cyberspace, Hart Publishing

Eeckhout, P. (2001), The EU Charter of Fundamental Rights and the Federal Question, 39 Common Market Law Review 947

Falce, V. (2011), La disciplina comunitaria sulle pratiche commerciali sleali. Profili ricostruttivi, in: A.M. Gambino (Ed.), Rimedi e tecniche di protezione del consumatore, 327, Giappichelli

Finocchiaro, G. (2017), Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali, Zanichelli

Finocchiaro, G. (2015), Da Google Spain a Schrems, 787, Diritto dell'informatica

Finocchiaro, G. (2014), I contratti ad oggetto informatico. Problematiche generali, in: F. Delfini / G. Finocchiaro (Eds.), Diritto dell'informatica, 605-614, Utet

Finocchiaro, G. / Delfini, F. (2014), Diritto dell'informatica, Utet

Finocchiaro, G. (2012), Privacy e protezione dei dati personali. Disciplina e strumenti operativi, Zanichelli

Finocchiaro, G. (1997), I contratti informatici, in: F. Galgano (Ed.), Trattato di diritto commerciale e diritto pubblico dell'economia, XXI, Cedam

Gambino, A. (1997), L'accordo telematico, Giuffrè

Halls, E. / Howells, G. / Watson, J. (2012), The Consumer Rights Directive – An Assessment of its Contribution to the Development of European Consumer Contract Law, European Review of Contract Law, 2, 151

[36] An alternative drafting technique for privacy and data-protection law could be based on the contextual privacy theory elaborated by the sociologist H. Nissenbaum. The theory of privacy in context is well described in Nissenbaum (2011); Nissenbaum (2010) and Nissenbaum (2004a, b), 119.

[37] In relation to personal-data protection, some authors have highlighted that the consent to personal data processing for the data subject is often based on a 'take it or leave it' mechanism (see Nissenbaum (2011), 35), while others have underlined the weak instantiation of choice. See Cate (2006).

Hesselink, M. (2007), European Contract Law: a Matter of Consumer Protection, Citizenship or Justice?, European Review of Private Law, 15, 323
Kuner, C. (2007), European Data Protection Law-Corporate Compliance and Regulation, Oxford University Press
Lord Goldsmith, Q.C. (2001), A Charter of Rights, Freedoms and Principles, Common Market Law Review, 38
Luzak, J. (2015), Passive Consumers vs. The New Online Disclosure Rules of the Consumer Rights Directive, Centre for the Study of European Contract Law, Working Paper Series 2
Luzak, J. / Mak, V. (2013), The Consumer Rights Directive, Working paper, available at: www.csecl.uva.nl
Macario, F. (1997), La protezione dei dati personali nel diritto privato europeo, in: V. Cuffaro / V. Ricciuto (Eds.), La disciplina del trattamento dei dati personali, Giappichelli
Mankowski, P. (2005), Information and Formal Requirements in EC Private Law, European Review of Private Law, 6, 779
Manzella, A. / Melograni, P. / Paciotti, E. / Rodotà, S. (2001), Riscrivere i diritti in Europa. Introduzione alla Carta dei diritti fondamentali dell'Unione europea, Mulino
Micklitz, H.W. (2012), Do Consumers and Businesses Need a New Architecture of Consumer Law?, EUI Working Paper law, 32, 266-367
Moerel, L. (2011), Back to basics: When Does EU Data Protection Law Apply?, International Data Privacy Law, 2, 92-110
Nissenbaum, H. (2011), A Contextual Approach to Privacy Online, Dœdalus
Nissenbaum, H. (2010), Privacy in Context: Technology, Policy, and the Integrity of Social Life, Stanford University Press
Nissenbaum, H. (2004a), Academy & the Internet, Monroe E. Price
Nissenbaum, H. (2004b), Privacy as Contextual Integrity, 79 Washington Law Review, 119
Smedinghoff, T. J. (1999), Electronic Contracts and Digital Signature: an Overview of the Law and Legislation, Practicing L. Inst. 125, 140-150
Smedinghoff, T. J. (1996), Online Law: the Legal Guide to Doing Business On The Internet, Addison-Wesley Developers Press
Turow, J. / Feldman, L. / Meltzer, K. (2005), Open to Exploitation: American Shoppers Online and Offline, Annenberg Public Policy Center, University of Pennsylvania, available at: http://www.annenbergpublicpolicycenter.org/Downloads/Information_And_Society/Turow_APPC_Report_WEB_FINAL.pdf
Twigg-Flesner, C. (2012), A Cross-Border-Only Regulation for Consumer Transactions in the EU – A New Approach to EU Consumer Law, Springer

Additional Sources

Article 29 Data Protection Working Party, Guidelines on the Implementation of the Court of Justice of the European Union Judgment on Google Spain And Inc V. Agencia Española De Protección De Datos (Aepd) And Mario Costeja González", C-131/12, adopted on 26 November 2014 (14/EN WP 225)
European Commission, DG Justice, DG Justice Guidance Document Concerning Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and June 2014 of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, June 2014, 37, available at: http://ec.europa.eu/justice/consumermarketing/files/crd_guidance_en.pdf

European Commission, Commission Staff Working Document Accompanying the Proposal for a Directive on Consumer Rights Impact Assessment Report, available at: http://ec.europa.eu/consumers/archive/rights/docs/impact_assessment_report_en.pdf

European Commission, Commission Staff Working Document, Accompanying Document to the Proposal for a Directive On Consumer Rights, Annexe, available at: http://ec.europa.eu/consumers/archive/rights/docs/proposal_annex_en.pdf

European Commission, Special Eurobarometer 359, Report on Attitudes on Data Protection and Electronic Identity in the European Union, June 2011, available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

Part IV
Personal Data, IP, Unfair Competition and Regulation

The Right to Data Portability and Cloud Computing Consumer Laws

Davide Mula

Contents

1 Cloud Computing Services 397
2 Cloud Services Contracts 399
3 The Standardisation Process of Cloud Service Contract Clauses 400
4 Lock-In and Right to Data Portability 403
5 The Well-Being of the Consumer Through a Holistic Legislative Approach 405
6 Conclusions 407
References 408

Abstract This paper examines the interactions between cloud service contract law and data-protection regulation in order to highlight the role that the latter plays in protecting consumers. The analysis aims to make it possible to understand whether and to what extent the European legislature has also influenced the regulation of cloud computing services by following a holistic approach in the adoption of the General Data Protection Regulation.

1 Cloud Computing Services

Telematics and the advancement of computer equipment, in particular mobile terminals such as netbooks, tablets and smartphones, which are characterised by small size, large-capacity connections to the network, but limited internal storage capacity, have led users—initially mainly for professional reasons and, later, also for personal reasons—to employ system data management telematics that enable them

Davide Mula is a lecturer in Data-protection and Biotechnologies Law, Legal Informatics and in Information and Communication Law (European University of Rome) and a fellow of the Italian Academy of the Internet Code.

D. Mula (✉)
European University of Rome, Rome, Italy
e-mail: davide.mula@unier.it

M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law*, MPI Studies on Intellectual Property and Competition Law 28, https://doi.org/10.1007/978-3-662-57646-5_15

to store and process information remotely, in a delocalised manner through the Internet.

These technological advances have led to the growth of the cloud services market, which allows for delocalised and on-demand access to a shared system of computing resources (e.g. networks, servers, storage, applications and services) through which it is possible to share data and functions rapidly.[1]

European law does not yet contain a standard definition of cloud computing, although in the Opinion of the European Economic and Social Committee (EESC) of January 2012,[2] the main technical features that characterise this new document-management system were identified as follows:

- Dematerialisation: this involves ensuring that the configuration, location or maintenance of IT resources is as invisible as possible for users, whether they are private individuals or businesses.
- Ease of access: provided that there is Internet access, users can access their data and applications wherever they are using them and by whatever means they wish (via computer, tablet, smartphone).
- Dynamic scalability: the provider adapts the IT capacity provided in real time to the user's needs. This means the user is able to cover peak loads without needing to invest in IT resources that are under-utilised between two peaks.
- Pooling: the provider is able to ensure dynamic scalability by pooling IT resources between various users. The provider can thus achieve the largest and best possible pooling, using huge server farms made up of several thousand computers.
- Pay-on-demand: the user pays only for the IT resources actually used, i.e. in line with changing IT capacity needs. The terms of such contracts are still often somewhat ad-hoc in nature; however, they are becoming increasingly standardised.

Cloud services are normally classified as[3]:

- Software as a Service (SaaS). The capability provided to the user is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various user devices through either a thin user interface, such as a web browser (e.g., web-based email), or a program interface. The user does not manage or control the underlying cloud infrastructure, including network,

[1] See National Institute of Standard and Technology, U.S. Department of Commerce (2011), 6: 'Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models'.

[2] European Economic and Social Committee, (2012), 3.

[3] NIST (2011), 2. Further classification of services is outlined in particular by Bradshaw, S. / Millard, C. / Walden, I. (2010) on hardware and software infrastructure ownership and on the conditions of accessibility to the platform. According to this parameter it is classified as private cloud, public cloud, community cloud and hybrid cloud.

servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application-configuration settings.
- Platform as a Service (PaaS). The capability provided to the user is to deploy on the cloud infrastructure user-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The user does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
- Infrastructure as a Service (IaaS). The capability provided to the user is to processing, storage, networks, and other fundamental computing resources where the user is able to deploy and run arbitrary software, which can include operating systems and applications. The user does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

2 Cloud Services Contracts

A cloud computing services contract is a legal relationship under which a subject, as a supplier or provider, offers a service to a user to be accessed by means of an electronic connection, through which the user can archive and manage data and documents remotely.

From a legal point of view, this new technology is based on the manner in which it is used, which has changed from a traditional proprietary model to a new model founded on the provision of a service—as is clear from the wording of the above-mentioned descriptions, where the phrase 'as a service' appears in every one of the terms.[4]

The use of cloud services takes place through a mechanism centred on access, following a model which has already been clearly identified in economic literature and called 'access culture'.

In the absence of a legal framework outlining provider and user rights in the cloud services markets, the contract signed between the parties is the only source from which to understand how to regulate the cloud service provided.

Cloud service contracts are generally structured into four documents: (1) Terms of Service (ToS); (2) Service Level Agreement (SLA); (3) Acceptable Use Policy (AUP); and (4) Privacy Policy.[5]

[4] See Hon / Millard / Walden (2012b), 85.

[5] For a detailed survey and analysis of the terms and conditions offered by cloud computing providers see Bradshaw / Millard / Walden (2010).

The first document (ToS) defines the general clauses of the contract such as duration, costs, means of providing the service, termination and withdrawal clauses.[6]

The second (SLA) regulates specifically the qualitative and quantitative level of the service that suppliers are obliged to provide and maintain and users must pay for.

The third (AUP) covers the acceptable use of infrastructure to which the user has access and above all the circumstances in which the supplier can terminate or suspend the provision of services.

The last (Privacy Policy) describes the way in which the provider should use and protect the user's personal data.

The most important of these documents is undoubtedly the SLA, since it defines the object of the contract and the quality of the services provided, as well as giving objective and measurable technical parameters such as the length of *uptime* and *downtime* or latency time.

3 The Standardisation Process of Cloud Service Contract Clauses

As has already been seen above, in the absence of a clear legal definition of the rights of both parties in the provision of cloud services, the contract represents the main instrument for defining and regulating the way in which the services must be provided, also taking into account the non-territorial nature of the services—as in many cases the parties are of different nationalities.

In this context, in February 2013,[7] the European Commission's Directorate-General for Communications Networks, Content and Technology (DG CONNECT), set up a working group composed of all the stakeholders with the aim of identifying the standard clauses which must be present in a cloud services supply contract.[8] The

[6] Cloud service agreements are frequently signed by parties of different nationalities who normally include clauses concerning the relevant legislation applicable to the contract in this first document. See Mantelero (2012), 1221.

[7] European Commission Decision (2013), Recital 5: 'The Commission intends to facilitate stakeholder agreement promoting the use of safe and fair terms and conditions in cloud computing contracts between cloud computing service providers and consumers and small firms. The Commission should work towards this goal with the active involvement of stakeholders drawing on their expertise and experience in the cloud computing sector. For this purpose, the Commission considers it appropriate to set up a group of experts on cloud computing contracts between cloud computing service providers and consumers and small firms. The tasks of the group shall be complementary to the work of the Commission on model terms for cloud computing service level agreements for contracts between cloud providers and professional users'.

[8] The constitution of a working group was already announced by the European Commission in its Communication of 2012: 'The Commission will by end 2013: […] Task an expert group set up for this purpose and including industry to identify before the end of 2013 safe and fair contract terms and conditions for consumers and small firms, and on the basis of a similar optional instrument approach, for those cloud-related issues that lie beyond the Common European Sales Law'.

result of the working group was the publication of the Cloud Service Level Agreement Standardisation Guidelines (hereinafter: Guidelines)—a document which provides a framework for the contractual obligations in accordance with European law to be applied in contracts, which at the same time standardise the (above all) technical vocabulary to be used.[9]

The need to standardise contractual clauses came about due to the global nature of cloud computing and the consequent involvement of contractual parties based in different legal jurisdictions, which consequently raises the issue of different legal regulations applied to the relationship, in particular concerning the protection of personal data.[10]

Amongst the various documents that make up the cloud computing contracts, the working group focused in particular on the conditions contained in the SLA, as this was considered to be the most important document regulating the contractual relationship between the user and the cloud provider.

The working group, offering technical definitions to be used in the various types of contracts,[11] also examined the issue of levels of service. There are in fact various problems relating to the nature of the service regulated by the cloud contract regarding the exact fulfilment of the contract by the provider, since the notion of quality of service is characterised differently depending on the type of service provided.

The concept of the quality of service is still not clearly defined despite the use of the metric unit as a measure of quality, given that this can be measured either at the time of delivery or at the time of use.[12] Standardising the service levels which the providers of cloud services must comply with helps to improve clarity and increase the understanding of the SLA, in particular highlighting and giving information on the key concepts regulated in practice, in these documents.[13]

However, when outlining their scope of application, the Guidelines specifically refer in the preamble to 'cloud service customers (not being consumers)', hence excluding the direct applicability of the principles contained within it to contracts with consumers.

---

[9] Cloud Select Industry Group – Subgroup on Service Level Agreements (2014).

[10] As highlighted in the Guidelines, 'this initiative will have maximum impact if standardisation of SLAs is done at an international level, rather than at a national or regional level. International standards, such as ISO/IEC 19086, provide a good venue to achieve this objective. Taking this into account, the C-SIG SLA Subgroup, as the European Commission expert group, set up a liaison with the ISO Cloud Computing Working Group to provide concrete input and present the European position at the international level. The SLA Standardisation Guidelines will serve as a basis for the further work of the C-SIG SLA and for a contribution to the ISO/IEC 19086 project'.

[11] The Standardisation Guidelines on this point stress: 'Keeping the definition of service level objectives well-defined and unambiguous is important to ensure the effective standardization of cloud SLAs and to enable clear communication between cloud service providers and cloud service customers. As technology develops and new terminology is developed it will also be important to ensure definitions are up-to-date and consistent with an evolving cloud services landscape'. See European Commission (2012), Mula (2016a).

[12] See Mula (2016b), 148 and note 52.

[13] See Hon / Millard / Walden (2012b), 113.

On this point it should be highlighted that in no other EU legal text can a definition of 'customer' be found. European law, in fact, recognises only the figure of the 'consumer', understood as the natural person who purchases a product to satisfy a personal need not connected to any professional employment undertaken, and who is protected as a consumer, and that of the 'user', understood as a legal or natural person who purchases a good or uses a service to satisfy their own personal or professional needs, protected by virtue of the special nature of the goods or services purchased.[14]

By using a term which was unknown in EU law, the working group that formulated the Guidelines seems also not to have considered that, due to the nature of cloud computing services, the use of these services falls under the regulation of the application of the E-Commerce Directive (2000/31/EC)[15] rather than under the normative framework for the protection of consumers.

Recital 18 of Directive 2000/31/EC clarifies, in fact, that 'Information society services span a wide range of economic activities which take place on-line' and, of particular interest in this context, that 'Information society services also include services consisting of the transmission of information via a communication network, in providing access to a communication network or in hosting information provided by a recipient of the service'.

From the clear wording of the above Recital it is evident that cloud services can be listed alongside the services of the information society, which do not relate to the figure of the consumer or 'customer', but more properly to the notion of the user, who is protected not by virtue of the act of purchasing the service, but rather by the specific nature of the service itself that puts consumers and professionals on the same level.

Directive 2000/31/EC has, in other words, extended the application of consumer discipline to the hypothesis in which the contractor is in a position of contractual weakness due to the absence of an individual communication channel, as happens in the case of contracts concluded through access to an Internet website.[16]

In the light of the above, a distinction should be made, therefore, between the final user and the intermediate user of the cloud service, placing the latter amongst subjects who use IaaS and PaaS services to provide in turn their own services.[17]

The narrowing of the scope of application of the Guidelines, moreover, risks jeopardising the work done. Taking into consideration the nature of the instrument,

[14] See article 2, number 1), Directive 2011/83/Eu of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council.

[15] 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 (2000) 178.

[16] See Parisi (2012), 397; Clarizia (2012), 361; Gentili / Battelli (2011), 347; Minervini / Bartolomucci (2011), 360.

[17] As Papi observes (2013), 3, the more complete the service provided is, e.g. SaaS, the less possibility users have to modify the cloud service.

however, there is in any case no reason to suggest that the Guidelines should not be applied to consumers—indeed it is for these very consumers that the use of the definitions approved by the working group has proved to be the most useful result of the initiative.

The possibility of applying the regulatory indications contained in the Guidelines to consumers as well reveals its usefulness especially with regard to the listing of clauses whose inclusion was considered essential by the working group. These clauses cover, among other things, the terms and timing of assistance, as well as the arrangements for data portability for the resources installed on the platform by the user in case of withdrawal from the contract.

Among the clauses concerning the management of stored and processed data via cloud services the Guidelines highlight the importance of establishing specifically the necessity that upon termination of the contractual relationship the user is put in the position of being able to transfer their data to another location.

4 Lock-In and Right to Data Portability

One of the principal characteristics of cloud computing—that distinguishes it from previous models for the use of technologies—is the delocalisation of the information technology resources; in other words the material inaccessibility of the user to the infrastructure and the data. This means that even though the user has the right to access the infrastructure at any time, and despite being the sole owner of the data, users do not store the data themselves and they do not have autonomous access to it without going through the provider, even if this takes place automatically. It is the cloud provider that stores the data and is therefore the only one to have material access to it.

This is one of the main reasons why users are often diffident towards this new technology, as for them it means the loss of the material access to data and the possibility of encountering technical problems if they decide to go back to the internal management of data.[18]

The physical unavailability of the data, and the circumstances under which it is archived in a format that only the cloud provider is the owner of, expose the user to the so-called technological lock-in phenomenon.[19] This occurs every time a technological choice forces the user to use the same technology to continue to use the computer purchased or the data created or elaborated, unless they are willing to bear substantial costs to adapt the computer or the data to another technology.[20]

These conditions mean that in the case of a withdrawal or a termination of the contract it is not economically viable to transfer the data to a different supplier or,

[18] Marchini highlights this aspect: Marchini (2010), 101.

[19] The most well-known lock-in cases are Bell Atlantic - AT&T and Computer Associates – IBM; see Shapiro / Varian (1999), 106, and Miller (2007), 351.

[20] See Troiano (2011), 242-243 and Rizzo (2013), 101.

in any case, that the user is limited in the exercise of their right to take advantage of cheaper offers from competitors of the provider with whom they have the initial contract. For these reasons, the lock-in phenomenon represents a huge threat for consumers and an enormous advantage—but also a cost—for the suppliers.[21]

The lock-in risk can obviously be avoided through the use of a system which allows for the transfer of data from one operator to another without the user incurring substantial costs. This could be done through the implementation of open standards that make it possible to break free from proprietary mechanisms and hence make data and processing systems continuously interoperable.[22]

However, this option goes against the interests of the individual providers, especially those with greater negotiating power and market shares, who have no interest in making their own systems interoperable with those of their competitors.[23]

The risk, therefore, is that the user, who lacks contractual power, will become a victim of this kind of commercial behaviour—a risk which, when examined closely, the companies themselves run considering the non-binding instrument represented by the Guidelines.[24]

A source of protection of the private party's rights, however, can be found in the more recent regulation of personal data contained in Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR),[25] which will enter into force in 2018.

Article 20 of the GDPR, in fact, covers the rights of the interested party to 'data portability', or the right to transfer personal data from one electronic system to another without the hindrance of the controller of the data. As a precondition and with the aim of improving the data subject's access to their own personal data, the GDPR provides that 'the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format'.

It seems evident that the 'data' to which the European legislature is referring in the GDPR are personal data and not computer data as such. However, it should be observed that data commonly referred to as computer data in reality contain a huge amount of personal data[26] and that, especially in the new scenario with the advent of cloud computing, computer data cannot be excluded from this latter form of protection.[27]

---

[21] See Open Cloud (2010), 6.

[22] See Maggio (2016), 462.

[23] See Maggio (2016), 468.

[24] See Mula (2016b), 148.

[25] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR), OJ (2016) 119.

[26] Finocchiaro (2012), passim and Swire / Lagos (2013), 343, accept this argument, while Hon / Millard / Walden (2011), 213 are partially against.

[27] Reding (2011) said 'I want to give citizens better data portability. This means that if a user requests their information, it should be given to them in a widely used format which makes it

Recital 68 of the GDPR can also be cited here, which states: 'That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should not apply where processing is based on a legal ground other than consent or contract'.[28]

Article 20 of the GDPR in this way sets forth the right of the user to data portability regardless of the type of IT service used, hence extending the scope of the new Regulation concerning the processing of personal data and in practice producing the effect that was only a hypothesis in the Guidelines, which ideally limited it only to the benefit of companies, and furthermore omitted a specific power to insist on the insertion of the abovementioned clause in the contract. Article 20, therefore, while regulating the processing of personal data, results in a provision that exceeds the Guidelines mentioned above, by requiring providers to introduce this provision into the SLA.

5 The Well-Being of the Consumer Through a Holistic Legislative Approach

In the light of all that has been said above it is clear that the protection of the consumer in cloud service contracts with specific reference to data portability has been reached not through consumer regulations, but in the pursuit of other, different aims.

If the normative approach of the EU legislature regarding the regulation of the processing of personal data was initially that of defining a normative framework that allowed for the free circulation of data in order to encourage their use for economic purposes,[29] in the case given above the opposite process can be seen.

The European Union has in fact always been characterised as a structure based predominantly on economic goals. This has led to more attention and care being given to the fundamental freedoms of an economic nature. The logical consequence of this has been that some fundamental rights, starting with that of privacy,[30] have been protected above all due to the fact that they can be exploited for economic purposes.[31]

---

simple to transfer elsewhere. I strongly believe that users should not be bound to one provider simply because it is inconvenient to move their information from one service to another.'

[28] This Recital dispels the criticism of Hon / Millard / Walden (2011), 213.

[29] See Pizzetti (2009), 83; Ferrari (2012), 19; Panetta (2006), passim; Busia (2000), 476; Cerri (1995), passim.

[30] The right to privacy stems from the right to be let alone as described by Warren / Brandeis (1890), 193.

[31] See Niger (2006), passim and Alo (2014), 1096.

The subsequent proclamation in the year 2000, which entered into force in 2009 in the EU Charter of Fundamental Rights,[32] led the EU legislature to place greater focus on the fundamental rights under EU law and, of most interest here, to the call for the respect of private and family life and the respect of personal data, regulated by Articles 7 and 8, respectively.[33]

This change of approach permitted the introduction of a clause into the Treaty on the Functioning of the European Union aimed explicitly at the recognition of the right to the protection of personal data.[34] Article 16 of the TFEU thus provided the legal basis for the adoption of a normative framework for the processing of personal data and subsequently for the introduction of a Regulation on this matter.

This new approach has also shown its benefits on another level than that of protection of the individual.

The normative evolution described above in fact plays a part in the ever-changing technological scenario which, despite the efforts of the European Union, has seen American operators as the true protagonists in a context in which the natural environment for the provision of services is unconnected with the territory in which the provider is established and that takes on global dimensions both for technical and economic reasons.[35]

The delocalisation of the cloud service leads, in fact, to a naturally international dimension regarding contracts, which limits the true scope of consumer-protection regulations.[36]

It is here, therefore, that the protection of personal data becomes a vehicle for the rights of cloud service users—in the use of a holistic approach towards the protection of the individual/user. The right to data portability, moreover, can also be beneficial for companies lacking strong contractual power, in order to insist on the insertion of this clause into the cloud service supply contract. In fact, the provision in the contract of a 'private' space dedicated to the employees of the contracting company obliges the provider to consent to data portability. As a consequence, the provider will then have an incentive to allow the portability of all the information assets of the company and to identify alternative tools from that of lock-in technology in order to keep their clients.

The importance of this provision also stems from its direct applicability to all operators who offer cloud services to EU citizens, even if they are not established in EU territory.

Given that Directive 95/46/EC has proved unable to respond to the needs deriving from the globalisation of the markets and the challenge of the information and knowledge economy, the legislature has changed approach with the new Regulation,

[32] Charter of Fundamental Rights of the European Union, OJ (2000) 364.

[33] The development of the right to data protection is described by the Italian Academy of the Internet Code (2015).

[34] For the difference between the right to privacy and the right to data protection see Stazi / Mula (2013).

[35] See Hon / Millard / Walden (2012a), 4.

[36] See Hon / Hörnle / Walden (2012), 135.

substituting the model of distributed competences with a centralised model which is shared, clear and predictable.[37]

The GDPR transposes the case-law orientation regarding the notion of establishment that applies to every processing of personal data carried out through the activity of an establishment, or a data controller, or a data processor within EU territory, regardless of whether the processing occurs inside the EU and of the legal form of the branch or subsidiary.[38]

In line with the desire to widen the field of application of EU law—also with respect to the first proposal presented—the GDPR applies also to data processors not established in the EU, when the activity is connected to the offering of goods and services to said data subjects irrespectively of whether there is any payment connected with this.[39]

Under the GDPR a 'service' is understood to be offered to EU citizens if the processor attempts to offer the service provided in EU territory, even in the case where this is limited to providing access to these services. In order to evaluate the behaviour of the operators who are not established within the EU, attention must be paid to the language of the site and the currency accepted as payment for services, considering, for example, whether these are used in the territory of the third-party state in which the operator is established.[40] The evaluation parameters outlined by the EU legislature seem clearly to be susceptible to many different evaluations, to such an extent that it is possible to hypothesise that the Court of Justice will be inundated with preliminary questions on this point.

6 Conclusions

Considering all the above it is clear how the legislature has considerably widened the scope of application of the GDPR to include all cases in which, even if the operator is not established in the EU, it in any case processes the data of data subjects who are in the Union.

This widening of scope clearly brings ulterior benefits in terms of consumer protection. In fact, had the EU legislature adopted a norm with the same content as Article 20 within the regulatory framework for consumer protection it would in any case have led to a more limited application regarding what is or is not enforceable on non-EU operators through the protection of individual rights.

Nevertheless, the legislative instrument chosen has benefits for cloud providers as well. The choice to introduce the right to data portability through a Regulation allows for a uniform application of EU law in all Member States, which in turn

[37] See Balducci Romano (2015), 1619.

[38] See GDPR, Recital 22.

[39] See GDPR, Recital 23.

[40] See GDPR, Recital 23.

gives providers the possibility to interact with a single authority. The GDPR is in fact also characterised by the redefinition of the roles of national supervision authorities and the relations between these in the case of subjects operating in more than one Member State, through the definition of the figure of the lead supervisory authority, with the confirmation of the so-called one-stop-shop mechanism.

This mechanism is called on to operate only in the case of significant transnational conduct, either in static terms, linked to the plurality of locations of the company, or dynamic terms, meaning that the conduct leads to activities and specific effects that go beyond national borders. Such a mechanism is triggered, therefore, if the necessary grounds exist to qualify the behaviour of the operator as cross-border—i.e. that it is able to have a substantial influence on subjects resident in more than one Member State.

It is evident, moreover, that with the arrival of a harmonised legal framework the expectation that the enforcement itself of the fundamental right of the protection of personal data must conform to the principles of convergence, coherence and non-contradiction between national practices could not be ignored.

When, in fact, the processor of the data is established in more than one EU Member State or when the processor, even though established in one single State, processes the personal data of people belonging to more than one Member State, the supervision authority of the main establishment of the processor or the only State in which it is established takes on the role of the lead authority.[41]

This authority has the task of co-operating with the other authorities involved either due to the presence of branches of the data processor, or due to the involvement in the processing operations of its own citizens, or, lastly, after receiving a complaint about the operator. The lead authority is, in addition, the only interlocutor with the processor regarding the cross-border processing of data.

The European Data Protection Board set up in Article 68 of the GDPR, which replaces the Article 29 Working Party, will be given the task of defining the operating Guidelines for the resolution of any problems resulting from the application of the GDPR.

In the light of the above, it seems clear how the holistic approach considered here has great benefits not only for consumers, but also for all the operators in the cloud market.

References

Alo, E.R. (2014), EU privacy protection: a step towards global privacy, 22 Michigan State International Law Review 1096

Balducci Romano, F. (2015), La protezione dei dati personali nell'Unione europea tra libertà di circolazione e diritti fondamentali dell'uomo, Rivista Italiana di Diritto Pubblico Comunitario, 1619, Giuffrè

[41] See GDPR, Recital 124.

Bradshaw, S. / Millard, C. / Walden, I. (2010), Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services, Queen Mary School of Law Legal Studies Research Paper No. 63/2010, available at SSRN: http://ssrn.com/abstract=1662374

Busia, G. (2000), Riservatezza (diritto alla), Digesto delle discipline pubblicistiche, 476, Utet

Cerri, A. (1995), Riservatezza (diritto alla), Enciclopedia giuridica, 26, Treccani

Clarizia, R. (2012), Contratti e commercio elettronico, in: M. Durante / U. Pagallo (Eds.), Manuale di informatica giuridica e diritto delle nuove tecnologie, 361, Utet

Cloud Select Industry Group – Subgroup on Service Level Agreements (2014), Cloud Service Level Agreement Standardisation Guidelines, 24th June 2014, available at http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=6138

European Commission (2012), Communication "Unleashing the Potential of Cloud Computing in Europe", COM(2012) 529 final

European Commission (2013), Decision of 18 June 2013 on setting up the Commission expert group on cloud computing contracts (2013/C 174/04)

European Economic and Social Committee (2012), Opinion of the European Economic and Social Committee on "Cloud computing in Europe" (own-initiative opinion) – (2012/C 24/08)

Ferrari, G.F. (2012), La tutela dei dati personali dopo il Trattato di Lisbona, in: G.F. Ferrari (Ed.), La tutela dei dati personali in Italia 15 anni dopo. Tempo di bilanci e di bilanciamenti, 19, Egea

Finocchiaro, G. (2012), Privacy e protezione dei dati personali. Disciplina e strumenti operativi, *passim*, Zanichelli

Gentili, A. / Battelli, E. (2011), I contratti di distribuzione del commercio elettronico, in: R. Bocchini / A. Gambino (Eds.), I contratti di somministrazione e di distribuzione, 347, Utet

Hon, W.K. / Hörnle, J. / Walden, I. (2012), Data Protection Jurisdiction and Cloud Computing – When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3, 26 International Review of Law, Computers & Technology 129

Hon, W.K. / Millard, C. / Walden, I. (2011), The Problem of "Personal Data" in Cloud Computing - What Information is Regulated? The Cloud of Unknowing, Part 1, 1 International Data Privacy Law 211

Hon, W.K. / Millard, C. / Walden, I. (2012a), Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2, 26 International Data Privacy Law3

Hon, W.K. / Millard, C. / Walden, I. (2012b), Negotiating Cloud Contracts - Looking at Clouds from Both Sides Now, 16 Stanford Technology Law Review 79

Italian Academy of the Internet Code (2015), Position Paper "Criptazione e sicurezza dei dati nazionali", available at: www.iaic.it

Maggio E. (2016), Access to cloud distribution platforms and software safety, 14th International Conference of Global Business and Economic Development (SGBED), Montclair State University

Mantelero, A. (2012), Il contratto per l'erogazione alle imprese di servizi di cloud computing, Contratto e impresa, 1221, Cedam

Marchini, R. (2010), Cloud Computing. A Practical Introduction to the Legal Issues, 101, BSI

Miller, L. (2007), Standard Setting, Patents, and Access Lock-In: RAND Licensing and the Theory of the Firm, 40 Industrial Law Review 351

Minervini, E. / Bartolomucci, P. (2011), La tutela del consumatore telematico, in: D. Valentino (Ed.), Manuale di Diritto dell'Informatica, 360, ESI

Mula, D. (2016a), Il trattamento dei dati nel territorio dell'Unione e il meccanismo "one stop shop", in: S. Sica / V. D'Antonio / G.M. Riccio (Eds.), La nuova disciplina europea della privacy, 271-288, Cedam

Mula, D. (2016b), Standardizzazione delle clausole contrattuali di somministrazione di servizi cloud e benessere del consumatore, in: C.G. Corvese / G. Gimigliano (Eds.), Profili interdisciplinari del commercio elettronico, 133-150, Pacini

National Institute of Standard and Technology, U.S. Department of Commerce (2011), The NIST Definition of Cloud Computing, available at: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Niger, S. (2006), Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali, Cedam

Open Cloud (2010), Cloud Computing Use Cases, 6, available at: http://opencloudmanifesto.org/Cloud_Computing_Use_Cases_Whitepaper-4_0.pdf

Panetta, R. (2006), Libera circolazione e protezione dei dati personali, Giuffrè

Papi, M. Jr. (2013), Configurable Services in SaaS Environments Using Rules Engines, available at SSRN: http://ssrn.com/abstract=2339074

Parisi, A.G. (2012), Il commercio elettronico, in: S. Sica / V. Zeno-Zencovich (Eds.), Manuale di diritto dell'informazione e della comunicazione, 397, Cedam

Pizzetti, F. (2009), La privacy come diritto fondamentale al trattamento dei dati personali nel Trattato di Lisbona, in: P. Bilancia / M. D'Amico (Eds.), La nuova Europa dopo il Trattato di Lisbona, 83, Giuffrè

Reding, V. (2011), Building trust in the Digital Single Market: Reforming the EU's data protection rules, available at: http://ec.europa.eu/commission_2010-2014/reding/pdf/speeches/data-protection_en.pdf

Rizzo, G. (2013), La responsabilità contrattuale nella gestione dei dati nel cloud computing, Diritto Mercato Tecnologia, 101, Italian Academy of the Internet Code

Shapiro, C. / Varian, H.R. (1999), Information Rules: A Strategic Guide to the Network Economy, 106, Harvard Business Press

Stazi, A. / Mula, D. (2013), Le prospettive di tutela della privacy nello scenario tecnologico del cloud e dei big data, available at: http://e-privacy.winstonsmith.org/2013we/atti/ep2013we_03_mula_stazi_tutela_privacy_cloud.pdf

Swire, P. / Lagos, Y. (2013), Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique, 72 Copyright Maryland Law Review 335

Troiano, G. (2011), Profili civili e penali del cloud computing nell'ordinamento giuridico nazionale: alla ricerca di un equilibrio tra diritti dell'utente e doveri del fornitore, Ciberspazio e Diritto, 242-243, Mucchi Editore

Warren, S.D. / Brandeis, L.D. (1890), The right to privacy, 4 Harvard Law Review 193

The Interface Between Data Protection and IP Law: The Case of Trade Secrets and the Database *sui generis* Right in Marketing Operations, and the Ownership of Raw Data in Big Data Analysis

Francesco Banterle

Contents

1 Introduction 412
2 Personal Data Processing for Commercial Purposes 413
2.1 Direct Marketing 414
2.2 Profiling 414
2.3 Customers' Data Assignment 415
3 Protection of Personal Data Processed for Commercial Purposes as Trade Secrets 416
3.1 The Legal Regime of Trade Secrets Within the EU 416
3.2 Datasets of Customers' Information as Protected Trade Secrets 417
3.3 Trade Secret Requirements in the Trade Secrets Directive and Protection of Business Information Under Italian Case Law 418
3.4 Customers' Personal Data as Trade Secrets 421
4 Protection of Personal Data Processed for Commercial Purposes Under the Database sui generis Right 422
4.1 Database Right in Sets of Customers' Personal Data 425
5 The Interface Between Data Protection and Intellectual Property 427
6 Ownership of Raw Data in Big Data 428
7 The Case of Cloud and CaaS Solutions 429
7.1 Data Protection Aspects 429
7.2 Intellectual Property Aspects 435
7.3 Towards an Ownership Regime for Raw Data? 436
8 Conclusions 439
References 440

Abstract Data is the new oil. The value of personal data has changed marketing strategies and business models based on data analysis. This article analyses whether sets of personal data collected for commercial exploitation can be the subject matter

Francesco Banterle, PhD Intellectual Property Law – University of Milan.

F. Banterle (✉)
University of Milan, Milan, Italy

M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law*, MPI Studies on Intellectual Property and Competition Law 28, https://doi.org/10.1007/978-3-662-57646-5_16

of intellectual property (IP) rights, specifically trade secrets and the database *sui generis* right. The first part of the article provides a concise analysis of EU data protection laws and the requirements for processing data for commercial purposes. The second part examines whether lists of customers and profiling data can be protected as business information under the EU trade secret law, also recalling Italian case-law experience (Italy is a unique example, where trade secrets constitute full IP rights). The third part analyses whether a database consisting of personal data processed for marketing and profiling purposes can benefit from the database *sui generis* right regime. The last part of the article investigates the case of data ownership in the context of big data, particularly in relation to cloud platforms. This part elaborates the ownership regime set out by the intersection between data protection and intellectual property laws. Finally, the article asks which ownership regime is applicable to raw data that are not subject to privacy or intellectual property rights, in particular, whether raw data can be subject to a general property right.

1 Introduction

Information is the currency of the digital age, and data about customers are becoming a critical asset in markets for big data. Although this fact is often disregarded, people usually get free digital services by 'paying' with their data. Indeed, knowledge of customers' interests allows companies to predict trends and provide tailored products and more appealing advertisements. Emerging, fast-growing business models are increasingly counting on the availability of massive amounts of data about customers and their behavioural patterns in order to collect and monetise them.

A significant portion of this information is personal data relating to identifiable individuals. In this case, the exploitation of those data is subject to privacy laws. EU privacy laws allow the collection and use of customers' data for commercial purposes. However, these activities are highly invasive, and companies must respect a series of strict rules which often imply high costs.

When processing personal data for commercial purposes, companies create sets of customer data which may differ depending on the level of complexity of the processing activity, from newsletter groups to advanced profiling and behavioural advertising programs. Undoubtedly, this information is an intangible asset having economic value whose creation requires economic investments. Thus, it may be the subject matter of (intellectual) property rights (IPRs). In particular, the IPRs that are designed to protect data within the EU IP framework are trade secrets and the database right.

Determining the ownership regime on these sets of data will be assessed in light of the intersection between privacy and intellectual property. From a privacy law perspective, data subjects (i.e., customers) hold privacy rights over their data, while data controllers (i.e., companies processing data) act in a position of legal control

over their processing. On the other hand, IPRs may exist in these datasets, subject to certain limits. Furthermore, IPRs deal with data subjects' privacy rights (e.g., the right to object to data processing and portability). The particular nature of personal data reduces the absolute nature of IPRs existing in that information (as individuals retain privacy rights upon the use of their data).

Finally, when the concepts of privacy and intellectual property do not apply, determining the ownership of data is challenging. This issue is particularly relevant in the big-data market, where analytics and knowledge-extracting techniques make even raw data a valuable source of information. In particular, this is the case with cloud platforms, where cloud providers have an interest in analysing the data generated by their clients' activity (who may not have analytics strategies already in place). In this context, an interesting case relates to 'commerce-as-a-service solutions' (e-commerce cloud services), where both the cloud provider and the cloud client are interested in analysing the behaviour of the latter's customers. In the absence of contractual limitations regulating the ownership regime of those data, the question arises: who owns the data?

2 Personal Data Processing for Commercial Purposes

Processing personal data in the EU has been mainly regulated by Directives 95/46/EC (the Data Protection Directive) and 2002/58/EC (the ePrivacy Directive). The Data Protection Directive was recently repealed by the General Data Protection Regulation—Regulation EU/2016/679 (GDPR; collectively these are referred to as the "EU Privacy Laws").[1]

The EU Privacy Laws acknowledge the value of customers' data and their crucial importance in marketing strategies, allowing their commercial exploitation, subject to a series of conditions aimed at protecting data subjects' rights (i.e. fair processing). Processing personal data for commercial purposes can be divided into three main operations: (i) direct marketing, i.e., processing data to send commercial offers; (ii) profiling, i.e., the automated analysis of customers' habits to provide tailored services; and (iii) assignment of customers' data to third parties for their own marketing and use. Each operation amounts to a different purpose.[2]

[1] The ePrivacy Directive is planned to be revised by the European Commission to interact with the GDPR. See Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) of 10 January 2017, COM/2017/010 final - 2017/03 (COD).

[2] Article 29 Working Party (2016), 20.

2.1 Direct Marketing

Processing data for direct marketing mainly relates to unsolicited communications and generally requires the data subject's consent (the so-called opt-in mechanism). Marketing also extends to "hosted" communications, where an organisation sends unsolicited communication on behalf of other parties.[3]

Data subjects have the right to object to processing for marketing at any time and free of charge. Therefore, data controllers interested in marketing processing must implement proper unsubscribe or objection mechanisms to update data subjects' preferences.

2.2 Profiling

Profiling is the automated processing of personal data aimed at evaluating personal aspects of users' personalities and creating datasets of user profiles. Recital 24 of the GDPR explains the concept of profiling through online monitoring where "natural persons are tracked on the internet […] particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes". Profiles can be (i) predictive, generally created by inference from analysing and matching individual and collective user behaviour (e.g., by monitoring the contents they view); or (ii) explicit, created from personal data (e.g., data provided through a website registration) and connected to specific individuals.[4] However, the two categories can be combined, and predictive profiles can become explicit at a later time, when associated with other identifying data (e.g. after creating an account).[5]

Article 22 of the GDPR specifically regulates profiling operations part of an automated decision-making process.[6] Since in many cases profiling is done without the data subject's knowledge, the GDPR reinforces consent as one of its main legal

[3] Ibid. The ePrivacy Directive sets out an exception, introducing an opt-out mechanism (i.e., to unsubscribe from future marketing messages) allowed only for (i) using e-mail addresses already obtained by the data controller in the context of the sale of a product/service and (ii) direct marketing of its own similar products or services (Article 13). The GDPR adds that customers' data can be processed for direct marketing in light of the legitimate interest of the organisations, as an alternative legal basis to the data subjects' consent. In fact, the scope of this provision should not significantly differ from the opt-out mechanism illustrated above. See Article 29 Working Party (2014a) and Banterle (2016).

[4] Article 29 Working Party (2010a), 7.

[5] Article 29 Working Party (2007), 18-21.

[6] Profiling which may significantly affect individuals is permitted if based on (i) the data subject's explicit consent; (ii) a contractual relationship, or (iii) a provision of law. Profiling which does not significantly affect individuals can be based on other legal grounds, such as legitimate interest.

basis, in line with the ePrivacy Directive provisions on online tracking (Articles 6 and 9).[7] Consent must be specific and separate from that required for other purposes.[8] If valid consent is not given, data subjects have the right not to be subject to a decision based on profiling which "significantly affects" them.[9] However, as consent is no longer considered a sufficient guarantee, the GDPR imposes further measures: mitigation of risks, transparency, and control for data subjects. Indeed, data controllers must implement 'suitable measures'[10] to safeguard the rights of individuals and inform data subjects about the profiling criteria and possible consequences.[11] Finally, at any time data subjects can object to profiling activities based on their consent.[12]

2.3 Customers' Data Assignment

Data controllers may transfer customers' data to third parties for their own marketing. This processing is always subject to the data subject's consent, which will be separate from the consent for data controller marketing.[13] The categories of third parties will be specified in the privacy information.

Finally, the GDPR has dramatically increased sanctions for non-compliance with data protection law provisions (monetary penalties are now up to 4% of global annual turnover—Article 83). Therefore, processing data, particularly for commercial purposes, exposes the controller to serious risks and liabilities.

---

[7] Under the Data Protection Directive, Article 15 limited the possibility of automated individual decisions where (i) necessary for the performance of a contract; or (ii) provided by law. Articles 6 and 9 of the ePrivacy Directive provide that profiling for marketing or for the provision of value-added services must be based on the user's consent.

[8] See Recital 32 of the GDPR; this is also known as "granular" consent.

[9] The term "significantly affect" sounds obscure, however, and will need further guidance. It seems to suggest a minimum threshold, excluding the need for consent for profiling operations which would not have significant effects on individuals, as it may probably be the case of marketing decisions (unless a risk of discrimination exists). See Article 29 Working Party draft Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, of 3 October 2017, 17/EN WP 251, 11.

[10] Article 29 Working Party (2013a), 4, explains that suitable measures should comprise the usage of data-protection-friendly technologies and standard default settings, data minimisation, anonymisation or pseudonymisation, data security, and human intervention.

[11] See Article 13 of the GDPR.

[12] See Article 21 of the GDPR.

[13] Article 29 Working Party (2016), 20.

3 Protection of Personal Data Processed for Commercial Purposes as Trade Secrets

3.1 The Legal Regime of Trade Secrets Within the EU

The concept of trade secrets traditionally refers to technical know-how and business information. The nature of this protection is a subject of debate, however.[14]

Trade secrets are protected at the international level. In particular, Article 39 of TRIPS sets out standard minimum levels of protection of trade secrets as IPRs and provides a definition of the information that can be protected, focusing on three requirements: (i) secrecy; (ii) commercial value; and (iii) reasonable steps to keep the information secret.[15]

In spite of this international instrument, the trade secrets regime varies significantly at the EU level, and Member States have adopted different legal protection models. In fact, trade secrets are regulated with *ad hoc* legislation (Sweden); as types of intellectual property rights (Italy, Portugal, and only partially France); relying on unfair competition laws (Austria, Germany, Poland and Spain); and based on tort law (the Netherlands and Luxembourg) or on breach of confidence (UK, Ireland, and Malta).[16] Additionally, all jurisdictions rely on contract law.[17] A property approach is not followed by many Member States, apparently because it risks leading to excessive protection.[18]

In an attempt to reduce this fragmentation, the trade secrets regime has been recently regulated by Directive (EU) 2016/943 ("Trade Secrets Directive"). However, the aim of the Directive is not to introduce a full EU trade secrets regime, but rather to reach a partial harmonisation through a minimal standard of protection, leaving room for Member States to provide for more far-reaching protection.[19] Indeed, the Trade Secrets Directive does not impose the creation of forms of property rights over trade secrets. A property approach entails a protection of the information *per se*. The Trade Secrets Directive instead protects the information exclusively against misappropriation.[20] In fact, the Directive allows Member States

[14] See Aplin (2015), contemplating whether trade secrets are a form of property under the European Convention of Human Rights and the EU Charter of Fundamental Rights like other types of IPRs. Aplin argues that the Trade Secrets Directive rejects a robust property approach and instead adopts a more balanced unfair competition model, and welcomes this solution. For more on the concept of trade secrets as form of IPRs, see Bronckers / McNelis (2012) and Bently (2013).

[15] See Burri / Meitinger (2014).

[16] Baker & McKenzie (2013), 4.

[17] Torremans (2015), 28.

[18] Aplin (2014), 8. A risk of elevating trade secrets to the status of IPRs is that patents, and their related pro-competitive effects, would be replaced by trade secrets.

[19] See Recital 10 and Article 1 of the Trade Secrets Directive.

[20] See Recitals 14 and 16.

to maintain the type of protection desired as long as they implement requisites concerning uniform standard measures, remedies and exceptions.

3.2 Datasets of Customers' Information as Protected Trade Secrets

Due to the lack of a common legal framework, no uniform definition of trade secrets exists at the EU level. Many national trade secret regulations fail to provide a definition of what information may be protected.[21] Formal definitions of trade secrets can be found only in a few jurisdictions, while in most cases the notion is derived from case law.[22] Hence, despite certain common denominators (basically in line with Article 39 TRIPS), definitions diverge, and each jurisdiction has adopted different eligibility standards for information to qualify as a trade secret.[23] In this context, the Trade Secrets Directive aims at setting out a consistent definition of trade secrets. It evokes the concept of undisclosed information in Article 39 TRIPS and covers: (i) any information, including know-how, business information and technological information; (ii) that is secret; (iii) that has commercial value; and (iv) that has been subject to steps that are reasonable under the circumstances to keep it secret.[24]

The Trade Secrets Directive does not specifically define the concept of 'business information'. However, in explaining the scope of the trade secrets' protection it refers to 'commercial data' as information including business plans, market research and strategies, and information on customers and suppliers.[25] 'Information' refers to organised data.[26] The Impact Assessment which accompanied the proposal of the Trade Secrets Directive explicitly states that trade secrets may include information such as lists of clients/customers, internal datasets containing research

[21] Baker & McKenzie (2013), 4.

[22] Ibid, 5. According to the authors, specific statutory definitions can be found in Swedish trade secrets law; in the Italian and Portuguese codes of industrial property; in the unfair competition laws of Bulgaria, Czech Republic, Greece, Poland and Slovak Republic; in the civil code of Hungary and Lithuania; and in the Companies Act of Slovenia. The concept of trade secrets instead relies on case law in Austria, Belgium, Cyprus, Denmark, Estonia, Finland, France, Germany, The Netherlands, Ireland, Latvia, Luxembourg, Malta, Romania, Spain, and the UK. For instance, the German BGH has defined trade secrets as "any fact related to a business which is not obvious but only known to a limited group of people, that the holder wishes to maintain secret and which has economic importance" (e.g. in Kundendatenprogramm GRUR [2006] 1044, 1046), in: Sousa e Silva (2014).

[23] Baker & McKenzie (2013), 5.

[24] See Article 2 of the Trade Secrets Directive.

[25] See Recital 1 of the Trade Secrets Directive.

[26] Sousa e Silva (2014), 10.

data, or anything that may include personal data.[27] In fact, the concept of business information is broad and covers almost all kinds of commercial data.[28]

On the same ground, the European Data Protection Supervisor highlighted the relevance of information relating to individuals (and thus of personal data) to the concept of trade secrets[29] and considered lists of customer data as a type of business information, requiring broader consideration and protection of privacy rights within the Trade Secrets Directive.

In sum, customer information, such as lists of clients' contacts or datasets of customers' behavioural information, can be protected as business information.

3.3 Trade Secret Requirements in the Trade Secrets Directive and Protection of Business Information Under Italian Case Law

Among Member States, Italy is unusual in that it protects trade secrets as an IP right. Since it was issued in 2005, the Italian Industrial Property Code adopted a definition of trade secrets which strictly conforms with the concept of undisclosed information from Article 39 TRIPS and is already in line with the Trade Secrets Directive.

Under Italian case law, the scope of trade secret protection is broad and concerns any type of company information.[30] Specifically, business information may include: lists of clients,[31] whether actual or potential[32]; marketing techniques and datasets of profiled clients[33]; price and discount policies[34]; data relating to promotions and sale

[27] See Annex 21 of the Impact Assessment of the Trade Secrets Directive, 254.

[28] Torremans (2015), 30.

[29] EDPS (2013), 3.

[30] Scuffi / Franzosi / Fittante (2005), 450.

[31] Court of Venice, judgment of 16 July 2015, Riv. Dir. Ind., 2015, 437, stating that "customer lists can be protected as trade secrets even though competitors can easily discover the data of one or more customers, through participation in the events of previous years" (translated by the author).

[32] Court of Bologna, judgment of 8 March 2011, Giur. ann. dir. ind., 2011, 861.

[33] Court of Turin, judgment of 6 July 2012, Giur. ann. dir. ind., 2013, 1, 591 about information contained in the customer sheets including name, address, telephone number, indication of their willingness to buy wine, product preferences (deduced from the content of previous orders), and temporal fluctuations in purchases.

[34] Court of Venice, judgment of 16 July 2015, *supra* note 31; Court of Perugia, judgment of 23 January 2008, Giur. ann. dir. ind., 2008, 1, 675, stating that the misappropriation of a complete list of customers "with related identifying and sensitive data, prices charged to them, the suppliers' data, quotes of the pending negotiations" (translated by the author) violates the trade secret right. In the same sense, see Court of Modena, judgment of 20 April 2005, Giur. ann. dir. ind., 2005, 861, concerning "commercial information relating to customers, both with reference to the name and location and contractual conditions. Protection is granted also where the data is accessible by the competitor through market surveys" (translated by the author).

of products[35]; and in more general terms, customary relationships with clients[36] and suppliers.[37] A long debate concerned the possibility to protect mere e-mail lists as trade secrets. A first interpretation argued that to trigger trade secret protection, customer lists must contain contacts and further details about customers,[38] thus excluding simple mailing lists from protection. However, recent case law has emphasised the importance of digital marketing techniques and the value of customers' personal data, and also grants protection to mere e-mail groups.[39] The subject matter of confidential information should indeed be dynamic and should depend on economic and social factors. Thus, is worth noting that even whether social media contacts can constitute trade secrets is currently under debate.[40]

Regarding secrecy, the Trade Secrets Directive provides that the information, as a body or in its precise configuration, must not be generally known or easily accessible in that particular field. Italian Courts have construed secrecy as a relative rather than an absolute concept.[41] This means that secrecy is present notwithstanding the fact that a third party may re-create the confidential information as long as efforts in

[35] Court of Bologna, judgment of 27 May 2008, in Leggeplus, stating that "Article 98 of the Industrial Property Code refers to anything that may fall within the concept of know-how; then: information of a technical or commercial nature (regardless of its nature, whether it be technical-industrial company experiences or information of commercial character, or, again, information on the organisation, or, finally, financial, management or marketing information); this information must be related to a technical production or distribution process or organisational economic activity whose value is given by the savings achieved by the entrepreneur through its use; indeed, such information can also be individually accessible to the public with no inventive step, since it is its combination that gives it value and makes it attractive to third parties" (translated by the author).

[36] Court of Milan, judgment No. 6579 of 21 May 2014, giurisprudenzadelleimprese.it; Court of Brescia, judgment of 29 April 2004, Giur. ann. dir. ind., 2004, 1079: "secrets are those of technical but also commercial nature, namely the 'practices' established by the organization with its customers and suppliers" (translated by the author).

[37] Bologna Court of Appeal, judgment of 5 June 1993, in Giur. ann. dir. ind., 1994, 359, about suppliers' lists which included names and economic information.

[38] Court of Milan, judgment of 26 June 2015, docket No. 13999/2015, giurisprudenzadelleimprese.it.

[39] See Florence Court of Appeal, judgment of 9 May 2011, No. 635, Iusexplorer, stating that: "the importance of customer lists depends on peculiar characteristics: where this concerns a vast mass of customers, even a simple email list can become an important asset, conveniently grouping an agglomeration of individuals oriented towards a certain product or a certain class of products, which could be very difficult and costly to achieve by means of autonomous research" (translated by the author); Court of Venice, judgment of 16 July 2015, *supra* note 31; Court of Milan, judgment of 21 March 2014, No. 3958, giurisprudenzadelleimprese.it; Court of Bologna, judgment of 4 July 2008, Iusexplorer; Court of Florence, judgment of 26 November 2008, Giur. ann. dir. ind., 2008, 1, 1167.

[40] Surblytė (2016). See in the US, Cellular Accessories For Less, Inc. v Trinitas LLC, No. CV 12–06736 D, DP (SHx), 2014 WL 4627090 (C.D. California) Sept. 16, 2014.

[41] Guglielmetti (2003a).

time and economic resources are necessary,[42] for instance with searches or by reverse-engineering operations.[43]

Regarding commercial value, the Trade Secrets Directive states that it is either actual or potential, and may be present where its unlawful use is likely to harm the interests of the right holder (e.g. business interests, strategic positions or ability to compete).[44] The concept of economic value is therefore extremely general. Similarly, the Italian case-law interpretation of this concept is quite extensive. Information does not necessarily need to have value on the market or be licensed to third parties. Instead, the economic value is connected with significant utility to the holder, since creating this information requires an economic investment.[45] Many courts tend to identify this value as a competitive advantage. However, this positive effect can more simply result in an organisational situation that allows a company to operate on the market, thanks to its investment in developing such information,[46] i.e., obtaining these data enables firms to save time and money.

Finally, regarding reasonable steps, the Trade Secrets Directive does not offer any particular indications. The assessment is, however, factual and is to be conducted on a case-by-case basis. The word "reasonable" calls to mind a concept of proportionality.[47] This assessment should accordingly consider all the circumstances of the case (e.g. the company size and number of employees; activity and type of business; the marking of documents etc.). It is debatable how stringent this requisite should be. Italian Courts hold that security measures must be designed according to a principle of adequacy, to prevent information from being disclosed to third parties in the course of business or due to unlawful behaviours the company may reasonably expect.[48] Security steps may be internal, i.e., practical security measures, or

[42] Court of Milan, judgment of 14 February 2012, Giur. ann. dir. ind., 2012, 5859: "secrecy [...] does not require the information to be otherwise unreachable by the competitor, it being sufficient that its misappropriation involves a saving in time and costs compared to its autonomous acquisition" (translated by the author).

[43] Turin Court of Appeal, judgment of 28 January 2010, Giur. ann. dir. ind., 2010, 368.

[44] See Recital 14 of Trade Secrets Directive.

[45] Court of Bologna, judgment of 16 May 2006, in: Galli (2011), 906. The Court held that trade secrets are information useful or necessary to conduct a productive or distributive process. Their value is given by the savings and by the consequential utility caused by its use; Court of Brescia, judgment of 29 April 2004, in Giur. ann. dir. ind., 2004, 1079, holding that customer practices are "knowledge with clear economic value, to the extent that a competitor who acquires them may obtain significant savings" (translated by the author); Court of Milan, judgment of 14 February 2012, Giur. ann. dir. ind., 2012, 5859, stating that account must be taken of time efforts and human and economic resources required to the creation of that information, and the advantage on the market that the availability of a set of information produces.

[46] Court of Bologna, judgment of 27 May 2008, *supra* note 35, stating that "an economic effort to obtain the information will be necessary" (translated by the author).

[47] Sousa e Silva (2014), 20.

[48] Guglielmetti (2003a), 129. In the same sense Court of Bologna, 20 March 2008, in Giur. ann. dir. ind., 2009, 1, 367 stating that: "Business information […] must be kept secret by adopting the supervisory measures that experience has proven functional and constitutes an adequate barrier against violations that can be reasonably foreseen and fought" (translated by the author).

external, i.e., legal measures towards third parties.[49] Internal measures can be logistical or technical.[50] The former relate to organisational aspects, such as the functional division of information in separate areas with different or limited access criteria. The latter concern technical measures that restrict access to the information, e.g. passwords. In this regard, the use of individual credentials or other authentication to access client management software is often deemed sufficient.[51] With regard to legal measures, they mostly relate to contractual confidentiality obligations of third parties that may have access to the secret information.[52]

3.4 Customers' Personal Data as Trade Secrets

The particular nature of personal data processed for commercial purposes should play a role in assessing trade secret requirements.

Customers' personal data processed for commercial purposes are subject to strong presumptions of secrecy. First, a general duty of confidentiality is imposed by EU Privacy Laws on the data controller.[53] Indeed, disclosure of personal data (particularly those processed for commercial purposes, such as personal profiles and intimate details) would harm the individual's private sphere.[54]

Regarding commercial value, processing data for commercial purposes entails costs, in terms of IT infrastructure, human resources, and time investment (e.g. for collecting data subjects' consent). Therefore, the lawful acquisition of personal datasets and the consequential ability to exploit them constitute a precious asset.

---

[49] Court of Bologna, judgment of 27 May 2008, *supra* note 35, stating that trade secrets must be "subjected to segregation measures, with particular reference both to physical protection, ensured by adequate protection systems, and to legal protection, ensured by adequately informing the third parties who come in contact with the information of the trade secrets' confidential nature and the need to preserve it" (translated by the author).

[50] Court of Venice, judgment of 16 July 2015, *supra* note 31, stating that "regarding the adoption of measures to be considered reasonably adequate to keep the information secret, such measures can relate to any behaviour unequivocally incompatible with the entrepreneur's willingness to make information accessible to the public, such as pre-determination of the firm's circle of employees to which communication is permitted (in this case, only the sales agents working in the organisation of the event), and the establishment of direct measures to prevent leakage of information (in this case, the use of a personal password to access company computers and the software in use in the marketing and accounting units)" (translated by the author).

[51] Court of Venice, judgment of 16 July 2015, *supra* note 31; similarly, see Court of Bologna, judgment of 4 July 2008, Iusexplorer; and Court of Florence, judgment of 26 November 2008, Giur. ann. dir. ind. 2008, 1, 1167 which positively evaluated "that access to the management software and, more generally, to all commercial (list of customers and related sales conditions) and technical information […] is adequately protected by user names and passwords (and, in addition, the management program has additional protection)" (translated by the author).

[52] Court of Bologna, judgment of 27 May 2008, *supra* note 35.

[53] See Recital 39 of the GDPR.

[54] For example, disclosure of profiling data would harm individuals and is therefore prohibited.

Additionally, the value of customer data is becoming even bigger in the new data-driven economy, thanks to analytics techniques and their tremendous predictive ability.

Regarding reasonable steps, personal data processing is a risky activity. For this reason, EU Privacy Laws require that security measures be abided by. The GDPR increases security standards for processing data. For instance, it requires: (i) performing a risk assessment; (ii) adopting a series of security measures such as limiting access to personal data only to authorised employees[55]; (iii) adopting passwords or further access restrictions[56]; and (iv) segregating data processed for commercial purposes. In addition, the GDPR encourages the adoption of privacy by design solutions and further security mechanisms against data leaks, such as data encryption.[57] All the above are internal security measures.

Additionally, the GDPR imposes the execution of data processing agreements with outsourcers or third parties processing data on behalf of the controller (the so-called data processors).[58] In this case, the processor is prevented from any use of personal data which falls outside of the controller's instructions. Moreover, these agreements generally include further confidentiality measures.[59] Thus, they could be considered legal measures.

It is therefore reasonable to argue that adoption of privacy-by-design architectures or a proper implementation of the security measures required by EU Privacy Laws should facilitate compliance with the requirements for trade secret protection.

4 Protection of Personal Data Processed for Commercial Purposes Under the Database *sui generis* Right

Directive 96/9/EC (Database Directive)[60] introduced a new database right, the so-called *sui generis* right. It is a full property right[61] which protects investment made by database producers in obtaining, verifying and presenting database contents, and adds to copyright protection of databases.[62]

---

[55] See Article 29 of the GDPR.

[56] See Recital 39 of the GDPR.

[57] See Article 34 of the GDPR: data encryption exempts the data controller from notification duties in case of data breaches.

[58] The GDPR defines the processor as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".

[59] See Articles 28 and 30 of the GDPR.

[60] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ [1996] L 77/20.

[61] See Article 7 of the Database Directive, confirming that the database right can be licensed and transferred.

[62] While the *sui generis* right protects the investment made in the collection of the data, copyright protection of databases is based on the originality of the database, relating to the selection or

The Database Directive aims to regulate proprietary interests in the information market. The database right protects collections of data in any form, whether electronic, in paper form, online, or hybrid. The Database Directive sets out a broad definition of a database as a "collection of independent works, data or other material arranged in a systematic or methodical way and individually accessible by electronic or other means".[63] The contents of a database are information in the widest sense of that term.[64] Indeed, the nature of the data is irrelevant and can include any material such as tests, sounds, images, numbers, and data. The term "database" is defined in terms of its function, i.e., to store and process information.[65] Hence, the Database Directive requires contents to be arranged in a systematic or methodical way. Data must be organised and retrievable, and independent from each other.[66] Protection is also granted, as part of the database, to the indexation systems necessary to consult the contents.[67]

The database right arises if the investment is substantial.[68] The "substantial" requirement can be qualitative and/or quantitative.[69] "Investment" can be financial or professional and refers to any type of investment, whether in terms of human, technical and financial resources, or expending time, effort and energy.[70] The substantial investment can be in obtaining, verifying or presenting the content. "Obtaining" refers to collecting data, "verifying" relates to checking and updating the database, and "presenting" refers to communicating the data, and can involve for instance designing the user interface.[71]

The scope of the database right has suffered some uncertainties, however. A crucial question debated among national courts is whether a database derived from a main activity which entails creating data may be protected. The ECJ has decided a

arrangement of the contents, thus qualifying the database as the author's intellectual creation. Copyright protection of databases will not be analysed in this paper since it does not appear to be strictly related to classic databases for personal data processing, although it cannot be excluded that datasets of personal information can be eligible for such protection (especially in big data operations where the particular structure or design of the database or of the selection of data can be original).

[63] See Article 1 of the Database Directive; see also Derclaye (2008) and Davison (2003).

[64] Hugenholtz (1998).

[65] Derclaye (2005).

[66] The independence of the contents means that any piece of information is complete and separable without affecting its value. See Stamatoudi (2002).

[67] See Recital 20, even though this protection does not regard software.

[68] The database right lasts for fifteen years from the end of the year of completion of the database. The term can be renewed if a substantial change to the contents of the database occurs and there is a new investment. A regularly updated dynamic database should thus enjoy potentially indefinite protection.

[69] See ECJ, Fixtures Marketing Ltd v Oy Veikkaus Ab., C-46/02, ECLI:EU:C:2004:694, para. 38, stating that "a quantitative assessment refers to any means that may be numerically quantified, and a qualitative assessment refers to efforts that may not be quantified, such as an intellectual effort or a waste of energy".

[70] See Recitals 7, 39 and 40 of the Database Directive.

[71] Hugenholtz (1998).

series of cases about the interpretation of the term "obtaining".[72] All those cases concerned sports database fixtures (e.g. football matches used for betting). The common denominator of these cases is that the ECJ partially echoed the so-called spin-off doctrine[73] and rejected the database right protection where the investment concerns the 'creation' of data. On the contrary, the investment in obtaining the contents of the database must refer to the resources used to collect existing independent material into the database, and thus it must be directly attributable to the creation of a database. In other words, if the database is a by-product of the database maker's main activity, and the investment is dedicated to that activity (and not to the collection of existing data), the database *sui generis* right is excluded. Investment in creating data does not *per se* exclude database right protection. However, a substantial independent investment in a further and separate activity to arrange and process those data (or at least to verify and present them) is necessary.[74] Thus, the ECJ denied protection to collections of untreated single-source data and introduced a safeguard mechanism through the creation/obtaining distinction, similar to the idea/expression dichotomy in copyright law.[75] Some uncertainties remain, since it is often difficult to distinguish between creating and obtaining data.

In these cases, the ECJ did not address the question of what constitutes a substantial investment, although its rulings do suggest a general threshold: investment should not be 'minimal'.[76]

Hence, a general attitude of the ECJ has emerged, avoiding overprotection of the database *sui generis* right. However, in spite of the tendency to adopt stricter rules regarding eligible databases, the ECJ opts for a strong proprietary protection once protection requirements are met. The database right protects against substantial extraction or re-utilisation of part of the contents. Extraction is a broad concept. It

[72] ECJ, Dataco Ltd and others v Yahoo! UK Ltd and others, C-604/10, ECLI:EU:C:2012:115; ECJ, Fixtures Marketing Ltd v Organismos etc., C-444/02, ECLI:EU:C:2004:697; ECJ, British Horseracing Board v William Hill Organisations, C-203/02, ECLI:EU:C:2004:695; ECJ, Fixtures Marketing Ltd v Oy Veikkaus Ab, C-46/02, ECLI:EU:C:2004:694; ECJ, Fixtures Marketing Ltd v Svenska Spel AB, C-338/02, ECLI:EU:C:2004:696. For an analysis of these cases, see Derclaye (2005).

[73] According to the spin-off doctrine popular among Dutch courts and commentators, the database right accrues only in investments to which the production of the database is directly attributable. See Davison / Hugenholtz (2005); Derclaye (2005); Falce (2009).

[74] In para. 44 of the *Oy Veikkaus Ab* case (*supra* note 69) the ECJ held that: "finding and collecting the data which make up a football fixture list do not require any particular effort on the part of the professional leagues. Those activities are indivisibly linked to the creation of those data, in which the leagues participate directly as those responsible for the organisation of football league fixtures. Obtaining the contents of a football fixture list thus does not require any investment independent of that required for the creation of the data contained in that list".

[75] Davison / Hugenholtz (2005).

[76] In the British Horseracing Board case (*supra* note 72), the ECJ held that the investment in obtaining, verifying and presenting the contents (as opposed to the investment in their creation) was minimal, and therefore, the database was not eligible for protection. A similar reasoning is made in the three Fixtures Marketing cases (*supra* note 72).

refers to permanent or temporary and direct or indirect transfer of contents by any means or form, and the ECJ has endorsed this broad interpretation.[77]

4.1 Database Right in Sets of Customers' Personal Data

Database right protection seems applicable to sets of customers' personal data. Indeed, the definition of a database set out by the Database Directive embraces any type of data. Recital 48 states that the database protection is without prejudice to data protection law, thus recognising the possibility of databases including personal data. Indeed, the database right should not extend to contents which are subject to any existing right,[78] and therefore, it can coexist with privacy rights in respect of the information collected. Some national courts have confirmed that databases of customer data can be eligible for protection.[79]

In particular, sets of data processed for commercial purposes appear to meet all requirements for database protection. Lists of clients, contact information and behavioural profiles need to be systematically organised (e.g. in e-mail lists, personal or group profiles etc.), as well as accessed and retrieved through data management software. Customers' data are independent and have autonomous commercial value. However, there must be a specific substantial investment in collecting, verifying and/or maintaining the data.

In relation to databases of personal data processed for commercial purposes, whether the investment lies in the creation or collection is not a clear-cut issue. Technically, data controllers do not create personal data. Instead, they gather them from individuals.[80] Personal contacts are indeed provided directly by customers. Therefore, lists of clients and e-mail groups (data processed for direct-marketing purposes) are data "collected" rather than "created" by the data controller.[81] Additionally, collecting customer data often requires verification of the information gathered and a program to process and make the information accessible for marketing. Most importantly, as confirmed by national courts, processing data for marketing requires collecting users' consent and providing unsubscribe mechanisms, which are formalities connected to obtaining, verifying and updating data.[82]

---

[77] ECJ, Football Dataco v Sportradar, C-173/11, ECLI:EU:C:2012:642.

[78] See Recital 18 and Article 7(4) of the Database Directive.

[79] See *ex multis* England & Wales High Court, British Sky Broadcasting v Digital Satellite Warranty Cover Limited [2011] EWHC 2663 (Ch), 27 October 2011, where the Court held that Sky had *sui generis* property rights in a database of its customers; see also Court of Milan, judgment of 21 May 2014, No. 6579, giurisprudenzadelleimprese.it.

[80] Derclaye (2005), 10.

[81] EU Privacy Laws refer to the "collection" of data when gathering individuals' information.

[82] See British Sky Broadcasting v Digital Satellite Warranty Cover Limited, *supra* note 79, where the Court held: "Sky claim database right in three main databases: the Chordiant database, which is Sky's central customer database, and the FMS and IFS databases […] As at 31 December 2009 there were records for approximately 9.7 million subscribers. The details held for each subscriber

Some uncertainties may arise in connection with behavioural analysis. Profiling is an automated process, where software analyses customers' behaviour and generates profiling data. Behavioural information does not pre-exist. In most cases, data are self-generated and collected within the database as soon as the customer generates an action. Therefore, the creation and collection of data occur simultaneously. Yet whether the investment lies in the creation or the collection of data is debatable. In most cases, processing data for commercial purposes is a collateral activity of the data controller, aimed at boosting its main business. In fact, behavioural analysis may regard two aspects: (i) how the customer interacts with a service; and (ii) customers' purchasing histories. In the first case, data do not originate in the context of the main activity of the data controller. In addition, data are technically created by the customers and captured by the data controller. In the second case, although customers' purchasing data originate from the data controller's main activity, there is no investment in the creation of such data. At least an investment can be seen in efficiently collecting the data through analytics software. Additionally, the processing phase of those data is essential: without any collection, profiling data would have no use. Finally, setting up a profiling system requires: (i) methodically updating the data according to customers' behaviour or privacy preferences; (ii) a presentation of those data to allow their exploitation in marketing activities. Indeed, in processing data for commercial purposes, EU Privacy Laws require controllers to set up systems that record individual choices. Processing architecture should reflect

include name, address, telephone number, email address, details of their Sky equipment and installation date […] Sky's evidence is that they have invested over £250 million in the development of Chordiant. In addition, they spend over £300 million annually in obtaining and verifying the customer details in the databases. Much of this money is spent on call centres […] Sky also spends substantial further sums annually in maintaining both its database systems and the data they contain. […] Sky do not create new information when they enter a customer's details into the Chordiant database, they simply record pre-existing information in a systematic way. It might be argued that the installation date was created by Sky, but even if it that is right it does not assist the Personal Defendants with regard to information such as the customer's name, address and telephone number. Counsel for the Personal Defendants' argument would substantially deprive the contents of many databases of protection, contrary to the whole purpose of the Database Directive".

See also England & Wales High Court, Flogas Britain Ltd v Calor Gas Ltd [2013] EWHC 3060 (Ch), 16 October 2013: "The Flogas Database is a similar case of a collection of information which includes information that has previously existed, such as the names and addresses of the customers, as well as comments that may have been made by Flogas employees in the Memopad function of the system. Following British Sky Broadcasting, at the very least that information that previously always existed must not be regarded as information that has been created, and is therefore protected by the database right. I conclude therefore that there did exist a database right that was capable of being infringed".

Along the same lines England & Wales High Court, Forensic Telecommunications Services Ltd v West Yorkshire Police & Anor [2011] EWHC 2892 (Ch), 09 November 2011: "the skill, judgement and labour expended […] in ascertaining the addresses and collating them in the PM Abs List was not the right kind of skill and labour to attract copyright. As counsel for the Defendants rightly conceded in this paragraph, however, it was an investment in the obtaining of data which counts towards subsistence of database right. I would add that there is also evidence of verification of the data".

granular consent requests, update consumers' choices, register withdrawal consent or opt-out requests etc. Thus, an investment in the organisation and arrangement does generally occur, whether in terms of costs of software and IT equipment, human resources or time in collecting data.[83] The Explanatory Memorandum of the original proposal of the Database Directive observed that in many cases the arrangement of data in the database is the product of the data management software.[84] Thus, the investment connected to obtaining and operating such software for entering the data is relevant.[85]

In light of this, it is arguable that in profiling activities, the investment is directed to creating a database and to systematically processing such data rather than to creating it. For this reason, datasets of customer information should be protected under the database *sui generis* right.

5 The Interface Between Data Protection and Intellectual Property

Database and trade secret rights in sets of customers' personal data can be combined, giving rise to a strong protection mechanism. They can, however, also be limited by the particular (personal) nature of the data and must coexist with privacy rights.

Whilst it has been argued that privacy rights are not typical property rights,[86] data protection law undoubtedly pursues a public/social interest[87] (i.e. the fair processing of personal data). Consequently, EU Privacy Laws set out individual rights as well as regulatory provisions for processing personal data, such as: a general need to obtain granular consents; rights to access and update data; the right to object to the processing of the data for marketing purposes; data portability, etc.

On the other hand, EU Privacy Laws allow data controllers to exploit personal data for commercial purposes. As long as all data protection requirements are met (and subject to an accountability principle), data controllers have exploitation rights

[83] See Lavagnini (2016) and Cogo (2005), arguing that the activity necessary to collect the data subject's consent could amount to an investment in obtaining data.

[84] European Commission, Proposal for a Council Directive on the Legal Protection of Databases, COM(92) 24, final, 13 May 1992, 20.

[85] See Court of Milan, judgments of 4 March 2013, No. 7825 and No. 7808, Ryanair cases, Iusexplorer, which held that: "the investments made by Ryanair with New Skies and Open Skies software, quantified over 50,000,000 Euro, are not only related to data generation, but also to their external presentation to allow reservations, check-in, etc., which is one of the purposes of the *sui generis* protection" (translated by the author).

[86] Ubertazzi (2014); Purtova (2011); Corien (2006). Indeed, a property right includes two powers: the right to use a good and the right to exclude others from such use. Privacy rights do not include the right to use personal data (which resides in image rights, name rights, etc.), but rather the right to exclude others from using them.

[87] Sholtz (2001), addressing data protection violations in terms of social costs.

in those data. Thus, the position of control entails a sort of exclusive possession of data, which may also have competitive consequences.[88] Additionally, some commentators have argued that this control right is in fact enhanced by market failure, where information asymmetries between companies and users about the actual processing of data occur, and consumers face high monitoring costs.[89]

Hence, data protection and intellectual property laws create a complex ownership regime with respect to data. There is therefore an interaction between the two areas, which, however, may not cover all situations, as will now be examined.

6 Ownership of Raw Data in Big Data

The economic field where ownership of data is currently challenged is big data. The term "big data" refers to collecting and re-aggregating data on a large scale. It consists of a method of empirical inquiry and is essentially a new way of extracting insights from aggregated unstructured and structured information.[90] The concept of big data is often expressed by three features: volume, velocity, and variety.[91] Big data analysis is based on a large quantity of data captured by electronic devices from different sources that are connected to objects from everyday life and reveal users' intimate details, e.g., internet browsing, smartphone usage, social media connections and posts, online purchases, location data, etc. Additionally, the Internet of Things (IoT)[92] is increasing connectivity among devices tremendously and will multiply sources of data, thus increasing the analytics potential of big data.

Big data can serve both scientific and marketing research purposes. Two of the greatest values of big data lie in its ability to automatically monitor human behaviour and in its predictive potential. Indeed, big data can detect general trends and correlations in data as well as analyse or predict individual preferences, attitudes and purchase propensities. Indeed, much big data analysis does not need to connect data to specific individuals and is done anonymously. These analyses create datasets in which customers are divided into general behavioural categories. Companies purchase big data sets and cluster customers into categories to develop advanced marketing strategies.

Big data can, however, be more effective if based on identified individuals. Thus, big data has serious privacy implications. It can result in intrusively profiling people

[88] EDPS (2014).

[89] Sholtz (2001).

[90] Mattioli (2014), 539.

[91] ENISA (2015), 8.

[92] IoT is an innovative technology that "enables objects [by] sharing information with other objects/members in the network [and] recognising events and changes […] to react autonomously in an appropriate manner". See European Commission (2016a). The European Commission estimates that the market value of the IoT in the EU should exceed EUR one trillion in 2020.

and raises the risk of their becoming subject to automated decisions based on data analysis (the so-called 'dictatorship of data').[93] At the same time, this ability increases the value of sets of big data.

However, big data methods can add value to old data through data aggregation from different sources. Data reuse is one of the central sources of value,[94] and the ability to enrich data from multiple sources will become essential. In this context, even raw data hold value for the insights that can be extracted from them. Hence, ownership of information plays a central role.

7 The Case of Cloud and CaaS Solutions

One area where ownership of data is becoming important is cloud services, for instance outsourced e-commerce platforms, also known as "commerce as a service" solutions (CaaS). These platforms evolved from cloud-based services and allow companies to sell their product online without having adequate IT infrastructures and experience. In most cases, the provider is offering its CaaS solutions to many companies and is interested in carrying out big data analysis on the end users' behaviours to improve its services and marketing strategies, as well as in selling that marketing data analysis. However, whether the cloud provider is entitled to collect the data of its client's customers and use them for its own big data analysis is a subject of debate. Similarly, the grounds on which the cloud client could object to that processing and could claim ownership on those raw data may sometimes be unclear. In the absence of formal assignments in the cloud agreement, the answer may depend on various factors, mostly related to privacy and intellectual property aspects.

7.1 Data Protection Aspects

The ownership regime that applies to customers' information may depend on whether it qualifies as personal data, thus resulting in the application of EU Privacy Laws.[95]

[93] EDPS (2015), 8; in this scenario individuals are judged on the basis of what data indicate their probable actions may be.

[94] Mattioli (2014), 545.

[95] See Recital 26 of the GDPR.

7.1.1 The Concept of Personal Data

To this aim, personal data are any information concerning an identified or identifiable individual. On the contrary, anonymous data are not subject to EU Privacy Laws.[96] The concept of personal data is extensive, however.[97] In this regard, the GDPR states that to determine whether an individual is identifiable, all the means reasonably likely to be used (also by a third party) to identify that individual directly or indirectly must be considered.[98] In fact, even when a piece of information does not directly identify an individual, through data enrichment it can refer indirectly to him or her, thus becoming personal data.[99]

The monitoring of customer behaviour on web platforms is traditionally based on online identifiers, such as IP addresses,[100] MAC addresses[101] or mobile advertising

[96] See Recital 26 of the GDPR, which states that "the principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes".

[97] The GDPR defines personal data as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

[98] Recital 26 of the Data Protection Directive states that "to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person". The term "reasonably" refers to objective factors, such as costs and amount of time required for identification, in light of the technology available at that time.

[99] Article 29 Working Party (2013b), 30, stating that full anonymisation is difficult, and modern technologies allow re-identification of individuals. A different appropriate solution could, however, involve "partial anonymisation" or pseudonymisation (i.e., where data can only be linked to the individual if one is in possession of a decoding "key"), when complete anonymisation is not practically feasible. Whether partial anonymisation or de-identification is sufficient depends on the context. To this aim, it may be necessary to complement anonymisation techniques with further safeguards to ensure adequate protection, which include data minimisation as well as appropriate organisational and technical measures.

[100] The "Internet Protocol Address" (IP address) is a sequence of binary numbers that identifies a device connecting to a network that uses Internet protocol for communication and is assigned by the network. An IP address can be "static", or "dynamic". Dynamic IP addresses are assigned on a temporary basis, for each internet connection, and change on each subsequent connection. A dynamic IP address is not itself sufficient to allow identification of the user by a service provider. To this end, combination with other additional data is necessary. Conversely, "static" or "fixed" IP addresses are invariable and permit a continuous identification of the device. See Advocate General Campos Sànchez-Bordona in Patrick Breyer v Bundesrepublik Deutschland, C-582/14, ECLI:EU:C:2016:339.

[101] The "Media access control" (MAC) address is an alphanumeric number assigned by the manufacturer to a device that connects to a network. It works as a network address (or interface) and particularly as a Wi-Fi, Ethernet or Bluetooth identifier. It is a unique device identifier, since each device has a unique MAC address. MAC addresses of mobile devices are used by location analytics programs, usually through public "hot-spots" and WI-FI networks, in various locations (malls,

identifiers.[102] These data are serial numbers that identify the device being used. Although they do not immediately identify the individual who owns or operates the devices, these data can show some patterns of user behaviour. However, where associated with other pieces of information (e.g. a personal account), they can also directly or indirectly identify the user. Thus, these digital fingerprints are potentially personal data and may attract EU Privacy Laws.[103]

In other cases, analytics programs are based on pseudonymised data. Pseudonymisation is the process of replacing direct identifiers (e.g. the name or the user account) with codes or numbers, and it is aimed at collecting additional data relating to the same individual without the need to know his or her identity. However, if pseudonymised data can likely be re-traced it amounts to personal data.[104]

The assessment as to whether a potentially indirect identifier can be considered as personal has been traditionally conceived as a dynamic rather than a static evaluation. It used to depend mostly on the circumstances of the case, for instance on whether the identification was included in the ultimate purpose of the processing and/or on the means likely reasonably at the disposal of the data controller (or of third parties)[105] to identify the user (e.g. singling out, digital data cross-device collection and linkability, pseudonymisation keys, combining publicly available information e.g. on social networks, etc.).[106]

---

airports, etc.) mainly to create statistical reports with aggregated information. See Future of Privacy Forum 2013, which has issued a code of conduct for mobile location analytics, available at: https://fpf.org/wp-content/uploads/10.22.13-FINAL-MLA-Code.pdf. See Cormack (2013).

[102] Mobile advertising identifiers are alphanumeric codes randomly generated by modern mobile operating systems that are associated with the mobile device. The name of these identifiers depends on the operating system (e.g., "Google Advertising ID" for Android, "Identifiers for Advertisers" for iOS, and "Facebook App User IDs" for Facebook). Mobile advertising identifiers avoid the use of permanent device identifiers. See Network Advertising Initiative's Glossary, available at: www.networkadvertising.org.

[103] Article 29 Working Party (2007), 17. To determine whether a piece of information relates to an individual, account must be taken - among other factors - of the purpose of the processing. If the processing of the IP address is aimed at identifying the user, and if additional means likely reasonably to be used to identify the person are available, e.g., in the case of a request for a court to order the disclosure of personal details related to the IP address, the IP address is considered personal data (see ECJ, Patrick Breyer v Bundesrepublik Deutschland, C-582/14, ECLI:EU:C:2016:779). In other cases, for technical or organisational reasons, if the IP address does not allow identification of the users with reasonable means, it is not personal data.

[104] Article 29 Working Party (2007), 18, and Polonetsky / Tene / Kelsey (2016). In this case, although the activity amounts to a processing of personal data under EU Privacy Laws, the risk is low and allows flexible application of privacy rules. With regard to anonymisation, there are divergent interpretations at the EU level, see European Commission (2012).

[105] The phrase "likely reasonably" excludes cases where the access to supplementary data (that may indirectly identify the individual when combined with the IP address) is very costly in human and economic terms, or practically or technically impossible, or prohibited by law. In this sense, see the opinion of Advocate General Campos Sànchez-Bordona, *supra* note 100, para. 68.

[106] See Recital 26 of Data Protection Directive and Recital 26 of the GDPR, underlying the importance of the means "likely reasonable to be used" by the controller. If the processing is not aimed

However, in light of the increasing possibilities of identifying individuals, the GDPR has strengthened this approach. It has recognised that online identifiers, including IP addresses, may potentially identify users and create profiles, especially when combined with unique identifiers.[107] Therefore, the GDPR now includes online identifiers in the definition of personal data. Recently, both the ECJ and the Advocate General have endorsed a similar approach due to the increasing risk that individuals can be identified via IP addresses.[108] Accordingly, the European Data Protection Supervisor has argued that even big data should be considered 'personal',[109] because truly anonymous datasets are difficult to create.[110]

7.1.2 The Data Controller/Data Processor Relationship

The consequences of EU Privacy Laws' application are significant. The position of the parties plays a key role in determining legal control over personal data. Although in cloud services this aspect is highly debated, the primary position of control is generally attributed to the cloud client,[111] whereas the provider should act as a mere "data processor".[112] This means that the provider is not legally entitled to process

---

at identifying individuals, and technical measures to prevent identification are implemented, data would presumably not be considered as personal. See Article 29 Working Party (2007), 17.

[107] See Recital 30 of the GDPR.

[108] See ECJ, Patrick Breyer v Bundesrepublik Deutschland, *supra* note 103, and the opinion of Advocate General Campos Sànchez-Bordona, *supra* note 100, stating that if there is a practical possibility that the controller may obtain supplementary information to be combined with online identifier data to identify the users, online identifiers will be qualified as personal data. The possibility that the data may be reasonably combined with supplementary data itself transforms the IP address into personal data. According to the ECJ, the possibility to request a court to order the disclosure of personal details related to the IP address can be positively regarded to this end.

[109] EDPS (2015), 7.

[110] Article 29 Working Party (2014b), 3.

[111] The GDPR defines a controller as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data" (see Article 4).

[112] See Article 29 Working Party (2012), 8 and EDPS (2012), 10. In abstract terms, the cloud client is the data controller, since it determines the ultimate purpose of the processing and decides on the outsourcing. Both the Article 29 Working Party and the EDPS held that in certain cases, due to the complexity of the technical means used in the cloud environment, the cloud client may not be the only entity that can solely determine the purpose of the processing. Indeed, determining the essential elements of the means is not in the hands of the cloud client. Thus, the EDPS suggests qualifying the relationship between provider and client as co-controllership, particularly when the cloud client has no ability to negotiate the contractual terms of the cloud agreement. However, this assessment is not static, and if the cloud client is in a position to negotiate the cloud agreement, it can be qualified as the data controller under the circumstances. Indeed, the Article 29 Working Party (2010b and 2012) appears to support the qualification of the provider as data processor as a general rule, leaving the possibility of qualifying it as controller only in residual circumstances where the client has no ability to negotiate contractual terms. However, even in the case that the provider is qualified as co-controller, the situation does not change, and its position of control

data for its autonomous purposes, and particularly to process the cloud client's customer data without the client's consent.[113]

This aspect has serious effects on the possibility to carry out big data analyses on customer behaviour. Under the GDPR, big data analysis can particularly be based on one of the following grounds: (i) consent; (ii) secondary purpose exception; or (iii) legitimate interest.[114]

7.1.3 The Secondary Purpose Exception

Leaving aside the first ground,[115] a solution that might be argued is anonymising customers' data to exclude the applicability of EU Privacy Laws. However, anonymisation itself constitutes a further processing operation and must satisfy the requirement of "compatibility" for secondary processing.[116] Indeed, the GDPR allows processing for a second purpose that is compatible with the original purpose. This possibility is subject to a test, which is based on compatibility factors such as: (i) the relationship between the parties; (ii) the data subject's expectations; (iii) the possible consequences; and (iv) the adoption of appropriate safeguards, such as encryption or functional separation (through anonymisation or pseudonymisation).[117] These requirements would be difficult for the cloud provider to meet, particularly considering the absent relationship with end users[118] and the commercial nature of the

---

refers to the means of the processing only. This means that the provider is not entitled to autonomously determine the purposes of the processing. Additionally, the EDPS's opinion (suggesting a co-controllership scheme) was also based on the fact that the GDPR former proposal added to the definition of data controller the new element of "conditions" (i.e., a data controller is the natural or legal person who determines the purposes, conditions and means of the processing), which was not eventually included in the final version of the GDPR (see Article 4 of the GDPR). See also the "Data Protection Code of Conduct for Cloud Infrastructure Service Providers", of 27 January 2017, issued by the Cloud Infrastructure Services Providers in Europe, which qualifies the cloud provider as processor.

[113] Article 29 Working Party (2012), 11, states that the provider cannot process personal data of the cloud client's customers for further purposes. Thus, the purpose of the cloud provider is limited to the provision of storage services and security measures for data. See also Article 29 Working Party (2015), 9: "A data processor must act 'only on instructions from the controller' (Art. 17(3)) and should therefore configure its role as a mere leverage in the hands of the controller, with no involvement in the semantics of the processing and no margin of maneuver for any sort of further processing".

[114] See ICO (2014).

[115] Processors should not be entitled to ask consent of data subjects without controllers' authorisation.

[116] Article 29 Working Party (2014b), 3.

[117] See Recital 50 and Article 6(4) of the GDPR, and Article 29 Working Party (2013b).

[118] In addition, the data subject might arguably expect to have his or her data processed for statistical purposes by the controller and not by the processor. Moreover, functional separation and thus anonymisation are riskier if performed by the cloud provider, which can access large quantities of data of different cloud clients. For similar reasons, big data providers may not respect the principles of "necessity" and "data minimisation". Indeed, their big data analysis is performed by accessing

secondary purpose.[119] Moreover, the compatibility exception seems applicable only to the data controller, who is responsible for determining the initial processing.

Additionally, the GDPR sets out a research and statistics exception wherein processing data for those purposes can be considered compatible with the initial purpose.[120] Whilst this exception may apply to big data for scientific research, it seems applicable to marketing big data only in part. Basically, it applies where big data is not aimed at profiling individuals but rather at detecting mere general trends.[121] Apparently, that requirement could be met in the cloud context, where the cloud provider mainly aims at creating customer clusters. However, in this case, the exception also seems connected to statistical analysis directly carried out by the data controller.[122]

7.1.4 Legitimate Interest

The possibility of grounding the processing of personal data on a legitimate interest[123] is subject to a balancing test between the interest of the controller and the data subjects' rights.[124] In fact, the key factors to be considered when applying the

as much data as possible, from various sources, thus facilitating the collection of a larger variety of data than actually necessary, in view of future needs.

[119] Esayas (2015).

[120] See Recital 50 and Article 5(b) of the GDPR.

[121] Recital 162 of the GDPR states that "statistical purposes" means "any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results. Those statistical results may further be used for different purposes, including a scientific research purpose". However, "the statistical purpose implies that the result of processing for statistical […] or the personal data are not used in support of measures or decisions regarding any particular natural person". According to Article 29 Working Party (2013b), 29, statistical purposes cover different processing activities including "commercial purposes (e.g., analytical tools of websites or big data applications aimed at market research)". Thus, although the statistics exception could theoretically apply to big data, a distinction is made on whether the analysis (i) aims to detect general trends and correlations in the information; or (ii) is interested in individuals. Indeed, the second case concerns profiling of the data subjects, which might require an opt-in consent (with exceptions set out in Article 22 GDPR). Hence, only in the first scenario can the statistics exception apply.

Also in this case, however, the applicability of the exception to big data is subject to a rigorous and balanced application of a compatibility test, under the circumstances of the case. Indeed, to qualify a statistical purpose as compatible, further safeguards must be implemented, particularly the so-called "functional separation". This principle means that data used for statistical purposes must not be used to "support measures or decisions" that are taken with regard to the individuals concerned. To this aim, full or partial anonymisation are particularly relevant.

[122] As observed above, if the provider is acting as a data processor, it is not allowed to start a new processing operation.

[123] Interest is the stake or benefit that the data controller (or a third party) has in the processing of data. Similarly to the Data Protection Directive (see Article 7 lit. f), the GDPR excludes the legitimacy of controller's interest when it is overridden by the interests or fundamental rights of the data subject.

[124] Article 29 Working Party (2014b).

balancing test do not significantly differ from those of the compatibility test, and they tend to allow mostly big data for generic trends (limiting individuals' profiling). However, the decision to pursue a legitimate interest again lies exclusively with the controller.

In sum, EU Privacy Laws tend to prevent the cloud provider from performing big data analyses on its clients' customers. Only in two limited cases does the cloud provider seem entitled to analyse its clients' customer data: (i) if it is considered at least a co-controller; or alternatively, (ii) if the data to be analysed are originally anonymous (although this possibility will be affected by the GDPR).[125]

7.2 Intellectual Property Aspects

As illustrated above, the cloud client can benefit from the protection of sets of customer data processed for commercial purposes ensured in connection with trade secrets and the database *sui generis* right. In the absence of any contractual provision, however, to what extent these rights may prevent the cloud provider from collecting customers' data autonomously must be assessed.

First, both trade secret and database rights should protect "processed" data only. The database right protects data only after their collection. Indeed, the Database Directive aims to stimulate the development of processing systems rather than the creation of data. As a consequence, *sui generis* rights protect database contents as an organised set.[126] This protection is broad and applies against any kind of extraction, even if indirect, which leads to the reconstitution of the database as a whole, or at least a substantial part of it.[127] It also applies against the re-utilisation of the extracted contents in a different form or in combination with different materials.[128] Conversely, exceptions are provided exclusively for scientific research or in the case of unsubstantial extraction of databases made available to the public (Articles 8 and 9).

As the subject-matter of protection is not clearly defined, whether the database right can extend to raw data is a subject of debate. Recital 45 states that the database right does not constitute an extension of "protection to mere facts or data". However, the European Commission has acknowledged that the "*sui generis* right comes precariously close to protecting basic information".[129] Some commentators confirm the view that the database right does not extend to raw data[130] unless the reproduction

[125] Article 29 Working Party (2013b), 30.

[126] Koo (2010).

[127] ECJ, Directmedia Publishing GmbH v Albert-Ludwigs-Universität Freiburg, C-304/07, ECLI:EU:C:2008:552.

[128] Guglielmetti (2003b), 1237.

[129] European Commission (2005), 24.

[130] Lavagnini (2016), 1906 and Cogo (2009), 1255.

of those data is substantial or repeated[131] or the raw data are not available elsewhere.[132] In this last regard, protection of raw data in fact seems possible where the information is not available from other sources and the processing does not transform the information collected,[133] i.e. when raw and processed data coincide.

Whilst the cloud platform could be the sole source for one particular customers' data, big data has different processing methodologies.[134] Each one employs various criteria, software and algorithms, carries out autonomous elaborations, and creates different sets of patterns, often combining data from various sources. Therefore, the same raw data processed separately by the cloud provider and the cloud client can possibly give rise to different outcomes, thus probably further limiting database protection on raw data.

Similarly, trade secret protection is granted on some "processed" data, since secret information requires being subject to reasonable steps (to keep it secret). In the absence of an access restriction mechanism, data should not be protected. The outcome of big data analytics is generally stored in protected databases, while raw data are automatically generated by the platform and cannot be hidden from the cloud provider for functional reasons. Thus, in the absence of at least confidentiality provisions about raw data which are binding on the cloud provider, trade secret protection can be granted to processed data only. In any case, trade secret protection is not absolute, and it cannot prevent a third party from autonomously obtaining such information. Therefore, if raw information is not subject to security measures (at least of a legal nature), and its access is theoretically lawful, the cloud provider is free to process it.

7.3 Towards an Ownership Regime for Raw Data?

The residual hypothesis concerns ownership of customer information where privacy and intellectual property laws do not apply (e.g. where online behavioural data are anonymous and not processed yet).

---

[131] Lavagnini (2016), 1906.

[132] Colston (2001); the same view was expressed by the European Commission (1992), which stated that "if the information in question is available from other sources, there is no exclusive right in that information in favour of the creator of the database. If, on the other hand, the creator of the database is the only source of such information, licences for the commercial re-exploitation of the information must be granted on fair and non-discriminatory terms".

[133] Bertani (2000), 353. However, autonomous elaboration of raw data should give rise to an autonomous *sui generis* right.

[134] For instance, purposes can be different (trend analysis or individual profiling). Analysis can be done in real time (e.g. for fraud detection), near real time, or in batch mode (for trend analysis). The technique can be predictive, analytical, ad-hoc query, reporting, etc. See Mysore / Khupat / Jain (2013). See also ENISA (2015), 8, explaining three main parts of Big Data systems: "the data itself, the analytics of the data, and the presentation of the results of the analytics".

Big data and the IoT are stimulating the need to access data from different sources and to make secondary use of them for detecting data correlations. Therefore, even raw data have an economic value (indeed, the value of data resides in the information and insights that can be extracted from them). In light of this, the question is whether raw data (i) are public or private goods; and (ii) can be the subject of a general property right.

Property in data challenges traditional concepts of civil law.[135] Data are immaterial goods, which fall outside the classical scope of property.[136] Conversely, ownership of immaterial assets has been traditionally identified in intellectual property.[137] Yet information *per se* has a public good character and IP law tends to exclude the creation of property rights in it. As a confirmation, trade secrets (which may protect raw information) are rarely conceived as a property right. And even the database *sui generis* right is not designed to protect the creation of data.

Furthermore, property rights in goods are subject to a *numerus clausus* principle, preventing operators from creating previously non-existing property rights.[138] The same principle applies to intellectual property, where law must determine the relevant subject matter.[139] Thus, interests in *res incorporales* not included in existing property rights benefit from a limited protection, which is characterised by the absence of exclusivity.[140]

In this regard, to ensure protection in a similar "grey zone" between private and public goods, a proposed solution relies on the "material availability" of the immaterial good. That availability is derived from the property (or other rights) in the activity generating the immaterial good (e.g. the e-commerce service), and determines a privileged position of the owner that is entitled to enjoy the relevant immaterial benefits (including raw data).[141] Alternatively, protection of raw data can be inferred by a general principle occasionally affirmed by courts under which any outcome of an economic activity constitutes a good and its commercial exploitation is exclusively reserved to the entity that generated it.[142]

---

[135] Schneider (2015).

[136] Zeno-Zencovich (1989), 452.

[137] Van Erp (2009), 12, stating that "in many legal systems, the classical model of property law focused on corporeal objects, not on claims and intellectual property"; Pereira Dias Nunes (2015).

[138] Purtova (2011).

[139] Resta (2011), 22. Intellectual property is protected by Article 17(2) of the Charter of the Fundamental Rights of the European Union. The ECJ in Promusicae (ECJ, Productores de Música de España (Promusicae) v Telefónica de España SAU, C-275/06, ECLI:EU:C:2008:54, para. 62) confirmed that "the fundamental right to property […] includes intellectual property rights".

[140] Zeno-Zencovich (1989), 460.

[141] Resta (2011), 41, explicating this solution in relation to the image of goods.

[142] Resta (2011), 45, referring to a judgment of the Court of Rome, First instance, of 31 March 2003, Foro it., 2003, I, 1879, in relation to sport events; and the judgment of the BGH, of 25 January 1955, in BGHZ, 16 (1955), 172, which held that non-protectable know-how can, however, be subject to a general absolute right of the owner and unfair competition law protection.

In fact, an effective alternative protection for that raw information resides in unfair competition laws, which generally protect information lacking eligibility for trade secrets or *sui generis* rights protection.[143]

However, this framework conflicts with a modern emerging approach considering as a "natural" concept the ownership of any utility produced by a private activity where it has economic value.[144] Indeed, in light of the increasing role of immaterial assets, many are claiming that the concept of property is flexible enough to extend it to new objects and rights,[145] and to eventually allow commoditisation of data.[146]

The solution is not straightforward and requires legislative intervention. Indeed, the European Commission has recently initiated a discussion about data "ownership" in the EU legislative framework.[147]

A proprietary approach on general information has been criticised, however. It risks restricting access to knowledge and thus stifling innovation and progress.[148] The creation of a legal monopoly on raw data risks resulting in over-protection.[149] Indeed, in the big data context, data reuse, data enrichment, and access to multiple sources of information are essential. Particularly in the field of scientific research, the adoption of open data mechanisms should be stimulated. At the current stage, it is impossible to predict where value will be created. Access to data and the creation of knowledge should therefore be guaranteed.[150] Hence, the introduction of strong exclusive rights in data should be carefully assessed.

As illustrated above, the ownership regime determined by the interaction between intellectual property and data protection laws is not based on absolute exploitation rights. Ownership of data is connected to a form of possession derived from a situation of control over the data which may be unstable and has to be balanced with individuals' rights.[151] Alternative forms of protection are, however, available to fit business needs. Indeed, raw data can be factually protected by physical/technological access restrictions or by contract. The ECJ has confirmed that contractual freedom

[143] See for instance Article 99 of the Italian Industrial Property Code, which states that non-protectable trade secrets can, however, benefit from unfair competition law protection.

[144] Resta (2011), 28.

[145] Fairfield (2005); Schwartz (2004); Prins (2006).

[146] Purtova (2011), 56.

[147] See for instance the communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Building a European Data Economy, COM(2017) 9 final, Bruxelles, 10 January 2017, supporting the introduction of a new right in raw machine-generated data.

[148] Reichman / Samuelson (1997).

[149] See European Commission (2016b).

[150] Bambauer (2014).

[151] EU Privacy Laws refer to a concept of control over data. Not diversely, the Trade Secrets Directive defines the holder of a trade secret right as the entity "lawfully controlling" that information (Article 2). Trade secret protection is not absolute but applies against misappropriation or abuse only. The database right protects the interest of the person who takes the initiative and the risk of investing. However, protection has been limited to collection of data and creation of databases, excluding rights in the information *per se* and in its creation.

can regulate access to databases not protected by copyright or the database right, i.e. raw data.[152] An ownership regime determined by contract, intellectual property and privacy laws thus already results in a strong protection mechanism for data.

Some commentators have proposed a potentially less aggressive alternative to regulate access to raw data. They argue for a more balanced solution, to be regulated by unfair competition law and by introducing in certain cases an access system subject to fee to information to be used for commercial purposes.[153] Under a classical *liability rule*,[154] at least in sectors where open data needs exist, data owners would be granted an equitable remuneration while access to information would be guaranteed. Additionally, this system seems consistent with the new proposal for a Directive on copyright in the Digital Single Market.[155] Indeed, the proposal introduces a new exception for data mining, which aims at balancing copyright with the public interest in accessing information.[156]

8 Conclusions

This article has shown how the interaction between intellectual property and privacy laws creates an ownership regime on customers' data. Due to the personal nature of data, this ownership regime is not, however, based on absolute exploitation rights. Instead, ownership of data is connected to a form of control. A "grey zone" remains with regard to raw non-personal data, which mostly fall outside that protection. Ownership of those data as well as their public or private nature is questioned. Particularly, a property approach to raw data, as goods deriving from an economic activity, is debated. However, the creation of a legal monopoly on raw data gives rise to the risk of over-protection. Additionally, contractual freedom, technical access measures, intellectual property and privacy laws already configure an adequate mechanism to regulate data ownership in the big data market. Indeed, big data requires data reuse, data enrichment, and access to multiple sources of raw information. Thus, a flexible approach to data is welcomed. A compensatory mechanism could be investigated, at least in some sectors where the open data approach is to be stimulated, based on paid access to data for commercial use.

---

[152] ECJ, Ryanair Ltd v PR Aviation BV, C-30/14, ECLI:EU:C:2015:10.

[153] Ghidini (2015), 285. A proposed example is the model set out by Article 99 of the Italian Copyright Law, which regulates access to non-protectable technical data. See Reichman (1994), 2477, for a detailed description.

[154] Calabresi / Melamed (1972) and Bertani (2011), 210.

[155] Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market, COM (2016) 593, 14 September 2016.

[156] In particular the Proposal states that (i) data mining may be carried out in relation to mere facts or data not protected by copyright, with no authorisation (Recital 8); whereas (ii) data mining for research purposes on copyrighted material is not subject to any compensation (Recital 13).

References

Aplin, T. (2014), A Critical Evaluation of the Proposed EU Trade Secrets Directive, King's College London Law School Research Paper No. 2014-25, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2467946

Aplin, T. (2015), Right to Property and Trade Secrets, in: C. Geiger (Ed.), Research Handbook on Human Rights and Intellectual Property, Edward Elgar 421-437 (also available at: http://ssrn.com/abstract=2620999)

Article 29 Working Party (2007), Opinion No 4/2007 on the concept of personal data, 01248/07/EN WP 136

Article 29 Working Party (2010a), Opinion 2/2010 on online behavioural advertising, 00909/10/EN WP 171

Article 29 Working Party (2010b), Opinion 1/2010 on the concepts of "controller" and "processor", 00264/10/EN WP 169

Article 29 Working Party (2012), Opinion 5/2012 on Cloud Computing, 01037/12/EN WP 196

Article 29 Working Party (2013a), Opinion 03/2013 on purpose limitation, 00569/13/EN WP 203

Article 29 Working Party (2013b), Advice paper on essential elements of a definition and provision of profiling within the EU General Data Protection Regulation, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130513_advice-paper-on-profiling_en.pdf

Article 29 Working Party (2014a), Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 844/14/EN WP217

Article 29 Working Party (2014b), Opinion 5/2014 on Anonymisation Techniques, 0829/14/EN WP216

Article 29 Working Party (2015), Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing, 2588/15/EN WP 232

Article 29 Working Party (2016), Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), 16/EN WP 240

Baker & McKenzie (2013), Study on Trade Secrets and Confidential Business Information in the Internal Market, study prepared for the European Commission, Publication Office of the European Union, available at: http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_final-study_en.pdf

Bambauer, J.R. (2014), Is Data Speech?, 66 Stanford Law Review 57 (also available at: http://ssrn.com/abstract=2231821)

Banterle, F. (2016), Personal data processing for marketing purpose under the new GDPR: consent v legitimate interest and Recital 47 – first thoughts, IPlens.org, available at: https://iplens.org/2016/07/12/personal-data-processing-for-marketing-purpose-under-the-new-gdpr-consent-v-legitimate-interest-and-recital-47-first-thoughts/

Bently, L. (2013), Trade Secrets: "Intellectual Property" But Not "Property"?, in: H.R. Howe / J. Griffiths (Eds.), Concepts of Property in Intellectual Property Law, CUP, 60-93

Bertani, M. (2000), Impresa culturale e diritti esclusivi, Giuffrè

Bertani, M. (2011), Diritto d'autore europeo, Torino

Bronckers, M. / McNelis, N. (2012), Is the EU obliged to improve the protection of trade secrets? An inquiry into TRIPS, the European Convention on Human Rights and the EU Charter of Fundamental Rights, 34 European Intellectual Property Review 673

Burri, M. / Meitinger, I. (2014), The Protection of Undisclosed Information: Commentary of Article 39 TRIPS, in: T. Cottier / P. Véron (Eds.), Concise International and European IP Law: TRIPS, Paris Convention, European Enforcement and Transfer of Technology, Kluwer Law International (also available at: http://ssrn.com/abstract=2439180)

Calabresi, G. / Melamed, A.D. (1972), Property Rules, Liability Rules, and Inalienability: One View of the Cathedral, 85 Harvard Law Review 1089

Cogo, A. (2005), Note to Corte di Giustizia UE 9 novembre 2004, Case C-444/02, Fixture Marketing v. OPAP, 14 AIDA 415

Cogo, A. (2009), Note to Corte di Giustizia UE 9 ottobre 2008, Case C-304/07, Directmedia Publishing GmbH v Albert-Ludwigs-Universität Freiburg, 18 AIDA 374

Colston, C. (2001), Sui Generis Database Right: Ripe for Review?, 3 The Journal of Information, Law and Technology 1361-1369, available at: https://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_3/colston

Corien, P. (2006), Property and Privacy: European Perspectives and the Commodification of Our Identity, in: P.B. Hugenholtz / L. Guibault (Eds.), The future of the public domain, Kluwer Law International, 223-257 (also available at: http://ssrn.com/abstract=929668)

Cormack, A. (2013), Bins, MACs and Privacy Law, 15 August 2013, Jisc community, available at: https://community.jisc.ac.uk/blogs/regulatory-developments/article/bins-macs-and-privacy-law (last accessed: December 2016)

Davison, M.J. (2003), The Legal Protection of Databases, Cambridge: Cambridge University Press

Davison, M.J. / Hugenholtz, P.B. (2005), Football fixtures, horse races and spin-offs: the ECJ domesticates the database right, 27 European Intellectual Property Law Review 113

Derclaye, E. (2005), The European Court of Justice Interprets the Database Sui Generis Right for the First Time, 30 European Law Review 420 (also available at: http://ssrn.com/abstract=1133637)

Derclaye, E. (2008), The Legal Protection of Databases: A Comparative Analysis, Edward Elgar

Esayas, S.Y. (2015), The role of anonymisation and pseudonymisation under the EU data privacy rules: Beyond the 'all or nothing' approach, 6(2) European Journal of Law and Technology (also available at: http://ejlt.org/article/view/378/569)

European Commission (2005), DG Internal Market and Services Working Paper: First evaluation of Directive 96/9/EC on the legal protection of databases, Brussels, 12 December 2005, available at: http://ec.europa.eu/internal_market/copyright/docs/databases/evaluation_report_en.pdf

European Commission (2012), Evaluation of the Implementation of the Data Protection Directive, Annex 2, available at: http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_annexes_en.pdf

European Commission (2016a), Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination – Final Report, available at: https://ec.europa.eu/digital-single-market/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination

European Commission (2016b), Synopsis Report On The Contributions To The Public Consultation Regulatory Environment For Data And Cloud Computing, available at: https://ec.europa.eu/digital-single-market/en/news/synopsis-report-contributions-public-consultation-regulatory-environment-data-and-cloud

European Data Protection Supervisor (EDPS) (2012), Opinion on "Unleashing the potential of Cloud Computing in Europe", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf

European Data Protection Supervisor (EDPS) (2013), On the proposal for a directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-03-12_TRADE_SECRETS_EN.pdf

European Data Protection Supervisor (EDPS) (2014), Report of workshop on Privacy, Consumers, Competition and Big Data 2 June 2014, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Big%20data/14-07-11_EDPS_Report_Workshop_Big_data_EN.pdf

European Data Protection Supervisor (EDPS) (2015), Opinion 7/2015 Meeting the challenges of big data, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf

European Union Agency For Network And Information Security (ENISA) (2015), Big Data Security Good Practices and Recommendations on the Security of Big Data Systems, available at: https://www.enisa.europa.eu/publications/big-data-security/at_download/fullReport

Fairfield, J. (2005), Virtual Property, 85 Boston University Law Review 1047 (also available at: http://ssrn.com/abstract=807966)
Falce, V. (2009), The (over)protection of information in the knowledge economy. Is the Directive 96/9/EC a faux pas?, 4 Dir. aut. 602-628
Galli, C. (2011), Codice Commentato della proprietà industriale e intellettuale, Utet
Ghidini, G. (2015), Profili Evolutivi del diritto Industriale, Giuffrè
Guglielmetti, G. (2003a), La tutela del segreto, in: C. Galli (Ed.), Le nuove frontiere del diritto dei brevetti, Torino
Guglielmetti, G. (2003b), Commento all'art. 5, in: P. Auteri (Ed.), Attuazione della Direttiva 96/9 relativa alla tutela giuridica delle banche dati, CEDAM
Hugenholtz, P.B. (1998), Implementing the European Database Directive, in: J.J.C. Kabel / G.J.H.M. Mom (Eds.), Intellectual Property And Information Law, Essays In Honour Of Herman Cohen Jehoram, Wolters Kluwer, 183-200
Information Commissioner's Office (ICO) (2014), Big data and data protection, available at: https://ico.org.uk/media/1541/big-data-and-data-protection.pdf (last accessed: December 2016)
Koo, A.K.C. (2010), Database Right Decoded, 32 European Intellectual Property Review 313-319
Lavagnini, S. (2016), Sub art. 102-ter l.a., in: L.C. Ubertazzi (Ed.), Commentario Breve alle leggi su Proprietà Intellettuale e Concorrenza, CEDAM
Mattioli, M. (2014), Disclosing Big Data, Maurer Faculty Paper, 99 Minnesota Law Review 535 (also available at: http://www.repository.law.indiana.edu/facpub/1480)
Mysore, D. / Khupat, S. / Jain, S. (2013), Introduction to big data classification and architecture, available at: www.ibm.com (last accessed: December 2016)
Pereira Dias Nunes, D. (2015), The European Trade Secrets Directive (ETSD): Nothing New Under the Sun?, Lex Research Topics on Innovation No. 1/2015, available at: http://ssrn.com/abstract=2635897
Polonetsky, J. / Tene, O. / Finch, K. (2016), Shades of Gray: Seeing the Full Spectrum of Practical Data De-Identification, 56 Santa Clara L. Rev. 593 (also available at: http://ssrn.com/abstract=2757709)
Prins, C. (2006), When personal data, behavior and virtual identities become a commodity: Would a property rights approach matter?, 3:4 SCRIPTed 270, available at: https://script-ed.org/wp-content/uploads/2016/07/3-4-Prins.pdf
Purtova, N.N. (2011), Property in Personal Data: Second Life of an Old Idea in the Age of Cloud Computing, Chain Informatisation, and Ambient Intelligence, in: S. Gutwirth / Y. Poullet / P. de Hert / R. Leenes (Eds.), Computers, Privacy and Data Protection: an Element of Choice, Springer
Reichman, J.H. (1994), Legal Hybrids Between the Patent and Copyright Paradigms, 94 Columbia Law Review 2432-2558
Reichman, J.H. / Samuelson, S. (1997), Intellectual Property Rights in Data?, 50 Vand. L. Rev. 49
Resta, G. (2011), Nuovi beni immateriali e numerus clausus dei diritti esclusivi, in: G. Resta (Ed.), Diritti esclusivi e nuovi beni immateriali, Utet
Schneider, I. (2015), Big Data, IP, Data Ownership and Privacy: Conceptualising a conundrum, presentation in the themed session "IP Governance, Big Data, Data Ownership and Privacy" at the EPIP Conference "Intellectual Property in the Creative Economy", Glasgow, UK, 2-3 September 2015, available at: http://www.epip2015.org/big-data-ip-data-ownership-and-privacy-conceptualising-a-conundrum/
Schwartz, P.M. (2004), Property, Privacy, and Personal Data, 117 Harv. L. Rev. 2055 (also available at: http://ssrn.com/abstract=721642)
Scuffi, M. / Franzosi, M. / Fittante, A. (2005), Il Codice della proprietà industriale, 450, CEDAM
Sholtz, P. (2001), Transaction costs and the social costs of online privacy, First Monday 6/5, available at: http://firstmonday.org/ojs/index.php/fm/issue/view/133
Sousa e Silva, N. (2014), What Exactly is a Trade Secret Under the Proposed Directive?, 9 (11) Journal of Intellectual Property Law & Practice 923 (also available at: http://ssrn.com/abstract=2427002)

Stamatoudi, I. (2002), To what extent are multimedia works films?, in: F. Dessemontet / R. Gani (Eds.), Creative ideas for intellectual property, The ATRIP Papers 2000 – 2001, CEDIDAC

Surblytė, G. (2016), Data Mobility at the Intersection of Data, Trade Secret Protection and the Mobility of Employees in the Digital Economy, 65 GRUR Int. 1121; Max Planck Institute for Innovation & Competition Research Paper No. 16-03 (May 13, 2016), available at: http://ssrn.com/abstract=2752989

Torremans, P.L.C. (2015), The Road Towards the Harmonisation of Trade Secrets Law in the European Union, 20 Revista La Propiedad Inmaterial 27 (also available at: http://ssrn.com/abstract=2719015)

Ubertazzi, L.C. (2014), Proprietà intellettuale e privacy, Foro it., 3-16

van Erp, S. (2009), From 'Classical' to Modern European Property Law?, in Essays In Honour Of Konstantinos D. Kerameus, Sakkoulas / Bruylant, 1517-1533 (also available at: http://ssrn.com/abstract=1372166)

Zeno-Zencovich, V. (1989), Cosa, in: Digesto delle discipline privatistiche, Vol. IV, 438, Utet

Data as Digital Assets. The Case of Targeted Advertising

Guido Noto La Diega

To many it will occur, that an important means of doing good is thus opened up; and certainly good advices, on the most interesting subjects, might in this way occasionally be tendered. By some, such a system of advertising may be considered as rather disreputable

Fraser, W. (1834)

Contents

1 Introduction 447
2 The European Regulation of Targeted Advertising 455
3 European and International Self-Regulation of Targeted Advertising 462
4 Profiling, Direct Marketing and Algorithmic Decision-Making in the General Data Protection Regulation 468
5 "It's a Google Market": Adsense, a Recent Change to the Google Privacy Policy and Related Details 474
6 The Use of Digital Assets to Hinder Competition. Facebook and WhatsApp: From the Concentration to the Transfer of the Latter's User Data to the Former's IP Portfolio 481
7 Conclusions. A More Balanced Approach to Data as Digital Assets and the "Cooperative Charter on Online Behavioural Advertising" 489
8 Afterword. Of Chocolate Chips and Lavender Buds 493
References 494

Guido Noto La Diega is Senior Lecturer in Cyber Law and Intellectual Property at the Northumbria University; Director of 'Ital-IoT' Centre of Multidisciplinary Research on the Internet of Things; Fellow of the Nexa Center for Internet and Society; Co-convenor of NINSO The Northumbria Internet & Society Research Interest Group. Thanks to Eliza Mik for the valuable input and to Gintare Surblyte, Allison Felmy and Stella Wasielak for the thorough review. Responsibility for this chapter and the errors therein rests solely with the author.

G. Noto La Diega (✉)
Northumbria University School of Law, Newcastle upon Tyne, UK
e-mail: guido.notoladiega@northumbria.ac.uk

M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law*, MPI Studies on Intellectual Property and Competition Law 28, https://doi.org/10.1007/978-3-662-57646-5_17

Abstract Facilitated by the growth of cloud computing, artificial intelligence (e.g. machine learning), and big data (e.g. predictive analytics), new tracking and profiling techniques have been developed. They have enabled the rise of targeted advertising, that is the provision of advertisements tailored to the tastes and habits of the user who actually views them. If targeted advertising is effective, data protection laws still apply. Most regulations look at the phenomenon from the data protection perspective, whilst in this paper it is argued that a holistic approach should be sought. Indeed, intellectual property, competition law, and consumer protection come necessarily into play. A general idea in this paper is that one should treat the data as digital assets in the users' IP portfolio, thus leading the users to care more about the way their data are processed, shared, and sold. The starting point is the regulatory framework in Europe, with particular regard to the ePrivacy Directive. After critically analysing some international and European self-regulatory initiatives, case studies on Facebook and the use of data on sexual orientation will be presented to display how these systems work in practice if an Italian user files a claim with the Istituto di Autodisciplina Pubblicitaria that his rights have been violated. The chapter goes on to compare the Data Protection Directive and the General Data Protection Regulation, with a focus on direct marketing. Given that Google is the main actor of the targeted advertising world, it will be explained how the platform works and this work analyses its privacy policy to assess how data are treated with regard to this form of advertising. Before concluding, the chapter looks at targeted advertising from an intellectual property and competition law perspective. The chosen prism is the Facebook/WhatsApp concentration. The paper aims *inter alia* to evaluate whether the decision of the Commission, which authorised the concentration, would be different today, in light of the change in WhatsApp's privacy policy allowing the use by Facebook of certain data of WhatsApp's users. The chapter assesses, more generally, whether targeted advertising can be prevented or somehow regulated through the unfair commercial practices regime. This chapter concludes with a pragmatic proposal which aims to empower the users, yet strike a balance between their interests and rights and those of the ad networks, publishers, and advertisers (advertising companies). In general, one should recognise that the opt-in regime required by some regulators is not implemented by the targeted advertising companies; cumbersome regimes such as the notice and consent provided for by the ePrivacy Directive have been a failure. Therefore, one should impose on businesses a more reasonable opt-out mechanism, provided that the right to dissent is actually enforced (as opposed to the current practice of circumventing adblockers and similar tools) and that the information is clear, brief, and provided in an interactive and gamified way. The user has to be at the centre of the system, but data protection rules may not be the best means therefor.

1 Introduction

Advertising plays a critical role in the keeping the Internet free, especially by enabling the development of new business models that are flexible and dynamic enough to accommodate the constantly evolving needs of online users.[1] One need only mention the "freemium" model, whereby basic services are free thanks to advertising placements to third parties.[2] As recently observed with regard to the proposal for a new Copyright Directive, "access 'free' for users and the service draws its revenues, directly or indirectly, from advertising and user data".[3]

In recent years, facilitated by the growth of cloud computing, artificial intelligence (e.g. machine learning), and big data (e.g. predictive analytics), new tracking[4] and profiling[5] techniques have been developed. They have enabled the rise of targeted, or behavioural, advertising,[6] that is, the provision of advertisements that are tailored to the tastes and habits of the user who actually views them.[7] Users may

[1] Cf. European Commission, Case No. M.7217 – Facebook/ WhatsApp, 3 October 2014, para. 47, according to which the "vast majority of social networking services are provided free of monetary charges. They can however be monetised through other means, such as advertising or charges for premium services".

[2] Spotify is perhaps the most famous example of the "freemium" model. Amazon, LinkedIn, and Badoo are other noteworthy examples.

[3] European Commission (2016d), part 1/3, para. 5.2.1. This part refers to user-generated content on online platforms, but the idea applies to several (I would say most) online "free" services.

[4] On the use of high-frequency sounds to covertly track across a range of devices see Calabrese et al. (2015). For a solution based on semi-supervised machine learning methods see Díaz-Morales (2015). Cookie technologies may not be available in mobile applications. Therefore, the advertiser may, for instance, link the identifier used for advertising on mobile applications to an advertising cookie on the same device in order to coordinate ads across the mobile apps and mobile browser. For example, it is common experience that while using a free app (usually with in-app purchases), at some point the screen is occupied by an ad which, if one clicks on it (perhaps inadvertently), launches a web page in the mobile browser. Finally, one should keep an eye on Flash cookies, which cannot be deleted through the traditional privacy settings of a web browser. Reportedly, they have been used precisely as a tool to restore "traditional cookies" that were refused or erased by the data subject (Soltani et al. (2009), 1-8). See also Bauer et al. (2015).

[5] See Pandey / Mittal (2016), Fan et al. (2016), Kanoje et al. (2014) and Cufoglu (2014).

[6] Targeted advertising is sometimes referred to as behavioural advertising, but, strictly speaking, the terms are not synonyms. Indeed, the former can be considered as the genus and the latter as a species. There are several ways a prospective customer can be targeted: for instance, by analysing previous behaviour (behavioural advertising), the page or the content the user is displaying (contextual advertising) or known characteristics of the data subject (age, sex, location, etc.), or the information provided by the data subject at the registration stage (segmented advertising). Even though behavioural advertising can be more intrusive and can lead to the collection of more personal data, the issues arising from the different types of targeted advertising are similar. Hence, the paper will refer mainly to the concept of targeted advertising. Recently, it is becoming fashionable to call the phenomenon "interest-based advertising", but the change of names has practical consequences.

[7] There are countless ways to provide targeted advertisements, but for brevity's sake this chapter will not go into details. A good read is Yan et al. (2011), 213.

expect their browsing behaviour to be analysed to serve them with ads; therefore, they may not be surprised if the first thing they are shown when accessing Amazon is a group of goods similar to items they have previously viewed. What users may not be aware of, on the contrary, is the use of facial recognition techniques to mine their photos. For instance, a Northern California District Court[8] has recently considered that the Illinois Biometric Information Privacy Act is applicable to Facebook, which is likely to mean that the social network has breached the law by not requiring explicit consent for its activity of facial recognition.[9] The importance of photos for Facebook has been confirmed by its recent attempt to force[10] its users to download "Moments", a separate app to sync their private photos. The ordinary Terms of Service (ToS) and privacy policy apply to Moments, which means that Facebook will also leverage this kind of data in order to use "the information we have to improve our advertising and measurement systems so we can show you relevant ads".[11]

It is a common experience, for instance, to look for something on Google's search engine and then to see related advertisements popping up after logging in on Facebook. One is rarely aware of the quality and degree of tracking one is subject to. A tool that can improve such awareness is the LightBeam add-on. The below chart shows an experiment this author carried out. On 12 August 2016, at 16:45 GMT, after installing this add-on, the Mozilla browser was used to search for a video (The Chainsmokers—Don't Let Me Down ft. Daya) on YouTube. This simple operation, which lasted 20 s, made this author inadvertently interact with 19 third-party sites, mainly owned or controlled by Google (for instance, google.com, google.co.uk, content.googleapis.com, googlesyndication.com, googleusercontent.com, googlevideo.com, etc.). LightBeam showed 0.5 cookies being activated per second. After two hours of moderate activity this author interacted with 229 third-party sites by visiting 32 sites. Forty four cookies were from adform.net, 44 from smh.com.au 38 from Google's DoubleClick, 34 from adnxs.com. Some of these results came as a surprise, because this author had never (knowingly) visited Adform or Adnxs, which are, respectively, a global digital media advertising technology

[8] In re Facebook biometric - Information privacy litigation, Case 3:15-cv-03747-JD.

[9] In Italy, the *Garante della protezione dei dati personali* has authorised, subject to an explicit consent of the data subjects, the collection of biometric data for profiling purposes, following a request of a bank which wanted to profile its clients to prevent fraud. See *Garante per la protezione dei dati personali*, *Verifica preliminare. Trattamento di dati personali e biometrici basato sull'analisi comportamentale dei clienti di una banca in occasione della loro navigazione nell'area privata del sito web*, 9 June 2016 n. 256.

[10] Cf. Gibbs (2016). For the use of faces for advertising purposes see, for instance, Kopstein (2016).

[11] Facebook Data Policy, available at: https://www.facebook.com/policy.php. Facebook's strategy is quite clear. It is believed there is a common design behind 1) the new WhatsApp privacy policy allowing Facebook's access to WhatsApp's user data; 2) The separation of "Moments" and "Messenger" from the mother app; 3) The introduction of the "Live" function of Facebook; 4) The introduction of "Your Story" on Instagram; and 5) Instagram videos now recordable for up to 60 seconds (against the initial 15). Such functions incentivise users to produce more data and harness them (mainly) for advertising purposes.

company and a portal for publishers to the AppNexus online auction exchange used to sell advertising space. Nor had he been aware of DoubleClick's operations.

This experiment also allowed this author to discover which advertisers target him through Facebook. There are 11 "Advertisers with your contact info" and five "Advertisers whose website or app you've used".[12] The first group[13] is formed by advertisers who have paid to access some data of the user's profile. It is not entirely clear which data Facebook can sell the advertisers, since the only thing it declares not to share is the user's name and contact info,[14] But there is for sure access to sensitive data, such as gender data. Now, the use case presented is a bike seller who wants to narrow the target to all the women aged 18–35 who live in Sydney and are interested in cycling. What if one is a pharmaceutical industry that wants to target all the people in a certain hospital? This involves no personal data, only location data, yet they are nevertheless intrusive and from them one can easily infer health data, which are indeed sensitive. Take for example the case of women in abortion clinics targeted with anti-abortion ads.[15] No worries, though. Facebook tells us that we are in control over the ads thanks to a supposedly user-friendly tool.[16] Indeed, in the ads preferences page this author discovered he was being granularly profiled, his activities and interests have been broken down into 683 audiences (as the platform calls them), from the BFI London Film Festival to the Italian Social Movement, which was quite in dissonance with the actual political beliefs of this author.[17] Anyway, relying on an opt-out mechanism, this author had been tracked and profiled and the fact that the tool offered by Facebook is to opt out individually from each of the audiences does not seem fair.[18] Also, users should have the right to know on which basis people and companies that they do not know serve them with ads? After an afternoon spent in being redirected from one page to another, eventually this author landed on one which seemed to be more helpful.[19] There it was found out that this author's current (never autonomously chosen) ad preferences can be used to show him ads on apps and websites both on Facebook and off of the Facebook Companies. At the end of the day, this author decided to turn off the ads altogether.

[12] It is not straightforward how to find this information, which is available at: https://www.facebook.com/ads/preferences/.

[13] The second group (which includes, for instance, The Guardian) will not be analysed, because it less worrying, since one is likely to expect to be tracked by websites and apps with which one has interacted.

[14] https://www.facebook.com/about/basics/facebook-and-advertising/on-facebook/.

[15] See Coutts (2016).

[16] https://www.facebook.com/ads/preferences/.

[17] Facebook declares that this author has liked a page which was connected to the Italian Social Movement, but it does not let him see the page he has supposedly liked.

[18] There is also an ex-post mechanism. When the user views an ad, they can select "Why am I seeing this?" and they can choose to hide all ads from that advertiser. However, it is an opt-out mechanism, and the users should have right to prevent the ads from being shown, because viewing them can in itself create distress.

[19] https://www.facebook.com/settings/?tab=ads.

However, the popular social networking site discourages this choice by saying that who opts out will see "the same number of adverts, but they may be less relevant to you". Moreover, opting-out users may, nonetheless, "see adverts based on things that you do on Facebook". This could come as a surprise, because the things that users do can be defined as their behaviour and it does not make much sense that if one opts-out of the behavioural advertising, they will keep receiving ads based on the things they do, i.e. their behaviour. It seems impossible to opt out of Facebook targeted advertising: they have cleverly changed the name to "online interest-based ads". And when it comes to the law, changing names has practical consequences: it is not true that a rose by any other name would smell as sweet.[20]

Even though targeted advertising can benefit consumers,[21] most surveys show that users oppose the provision of this kind of advertising,[22] and even those surveys that evidence a positive approach towards this kind of advertising indicate that most users feel that it violates their privacy.[23] For instance, a Pew survey shows that 73% of the search engine users surveyed do not agree "with a search engine keeping track of your searches and using that information to personalize your future search results because [they] feel it is an invasion of privacy".[24] Moreover, 68% of all Internet users do not feel comfortable "with targeted advertising because I don't like having my online behavior tracked and analysed".[25]

On closer look, the complimentary character of the Internet is merely apparent. Indeed, not only is a price paid to the advertisers (albeit not by the end-users), but there might be a non-financial cost in terms of jeopardisation of privacy, competition, intellectual property, and consumer protection. As an experiment presented above shows, users who try to disable the cookies and the ads will find out that they are no longer able to access most of the online services. This proves that users of (apparently) free services are actually paying with their data and are acquiescing to being tracked and profiled. As has been observed with regard to the popular augmented-reality game Pokémon Go, "even gamers who never spend a cent on

[20] Side note. The experiment was conducted on 11 September 2016. The day after disabling all interest-based advertising this author accessed again https://www.facebook.com/ads/preferences/ and found that whereas the five "[a]dvertisers whose website or app you've used" had disappeared, the 11 advertisers with his contact information were still there. It is not clear on which basis they were still serving him with advertisements, if not on the basis of his supposed interests (or audiences).

[21] As pointed out by the European Commission (2016b), para. 3.5.5.1, with reference to Liem / Petropoulos (2016), "targeted Internet advertising in theory serves a useful informational role for consumers because they are able to see the ads that are related to their potentially unique interests [as] online platforms reduce the 'noise' of irrelevant advertising by enabling interest-based advertising that is based on users' personal data and demographic characteristics".

[22] See, e.g., Turow et al. (2009), 1-27; Marshall (2014).

[23] Ask Your Target Market (2011).

[24] Purcell et al. (2012), 1-42.

[25] Ibid.

in-app purchases or promotions are effectively producing information that becomes a commodity owned by Niantic".[26]

Intrinsically connected to other pressing issues, such as those related to cookies, profiling, and direct marketing, targeted advertising is no longer just the use of "information linked through cookies to create a profile of a user [in order to send] adverts which are likely to interest them,"[27] since the concept of the digital fingerprint goes clearly beyond cookies, and new tracking techniques such as cross-device tracking[28] are being developed every day.

If targeted advertising is effective, data protection and privacy laws will apply. Indeed, data are personal if they enable the identification of a person, regardless of the knowledge of the name of the person. For targeted advertising to be effective, the advertiser has to be able to single out a user and serve that user with bespoke commercial messages. If a user is singled out, data protection laws will apply.[29]

Data protection is just one of the prisms through which to observe targeted advertising. Indeed, targeted advertising shows how personal data have become a critical digital asset of the intellectual-property portfolio of a few strong actors[30] that

[26] Iveson (2016), who further observes "[t]his data could potentially be sold to third parties with an interest in targeted advertising". The Pokémon Go Privacy Policy, last updated on 1 July 2016, available at: https://www.nianticlabs.com/privacy/pokemongo/en/, is not clear about targeted advertising. It merely reads that "[s]ome third party services providers that we engage (including third party advertisers) may also place their own Cookies on your hard drive". Moreover, "we may use Web Beacons to deliver or communicate with Cookies, to track and measure the performance of our Services, to monitor how many visitors view our Services, and to monitor the effectiveness of our advertising". Clearer on this point is the Pokémon Privacy Policy, last updated on 19 April 2016, available at: http://www.pokemon.com/uk/privacy-policy/: "[w]e may collect and store your device's source IP address which may disclose the location of your device at the time you access the Services. Advertisements and certain content could be directed to you as a result of this data. In addition, in some cases the Services can deliver content based on your current location if you choose to enable that feature". It is also clarified that location data will be used to "[p]ersonalize the advertising you receive, including advertising based on your activity on our Sites or activity on third party sites and applications". It should be noted that Niantic, the owner of Pokémon Go, and Nintendo, the owner of Pokémon, developed the former in partnership. It is not clear whether the two companies may share the users' data. Moreover, Niantic spun out of Google in 2015, but it would be unsurprising if the former was indirectly controlled or at least influenced by the latter, given the generous financial support provided by Google and given that Niantic was born as a start-up within Google.

[27] Information Commissioner's Office (2011). The ICO distinguishes between non-targeted advertising, contextual advertising, and behavioural advertising. Even though contextual advertising could be considered to some extent, targeted, behavioural advertising will be the main focus of this paper.

[28] Cross-device tracking is crucial in an Internet of Things world. Consider, for instance, the use of high-frequency sounds to covertly track across a range of devices. Below, the chapter will give account of a Google privacy policy update that enables users to be tracked across devices (and services) via "My Account". In the field of advertising (especially mobile advertising), companies such as Rocket Fuel are developing solutions of cross-device optimisation ("Moment Scoring").

[29] Cf. Zuiderveen Borgesius (2016), 256.

[30] The relevance of targeted advertising for intellectual property is multifaceted. For instance, alongside the data themselves as assets (which can be transferred from the data subjects to the data

can leverage them in order to, on the one hand, carry out potentially unfair commercial practices, and on the other hand, turn the users into digital labourers and carry out discriminatory policies of targeted pricing, today tackled by the European Commission in the context of the Digital Single Market Strategy.[31] One of the solutions suggested here is to treat data as digital assets in the IP portfolio of consumers, as a way to lead them to understand the importance of their data, without necessarily preventing any kind of aware economic exploitation of these assets. There are several indicia of the current transformation of data into digital assets. This is underpinned by an understanding of privacy no longer as a human right (static and non-transferable), but as property (dynamic and transferable). Data portability, as introduced by the General Data Protection Regulation (GDPR),[32] is probably the clearest example of this development. Accordingly, data controllers (e.g. Facebook) are obliged to transfer the personal data to the data subject who provided them "in a structured, commonly used and machine-readable format."[33] Moreover, the data subject has "the right to transmit those data to another controller."[34] The shift towards data as digital assets was confirmed amongst others by the recent regulation on cross-border portability of online content services.[35] Indeed, the regulation does not allow the licence, communication, transfer, sharing, transmission and disclosure of personal data to the online content service provider[36] (e.g. Netflix when accessed by a German subscriber temporarily in England). Thus, *a contrario*, the regulation confirms that, outside this specific context, personal data can be licensed like any other intellectual property right.[37] Users would better realise the value of their data if they had to license them, rather than accept a privacy policy. In a draft regulation

controllers and to third parties), the algorithms used to analyse the users' behaviour are usually covered by trade secrets or related tools. On the problem of accountability in machine learning algorithmic decisions see Reed, Kennedy, and Nogueira Silva (2016).

[31] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "A Digital Single Market Strategy for Europe", COM/2015/192 final.

[32] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR), OJ [2016] L 119/1.

[33] GDPR, Article 20 (1).

[34] GDPR, Article 20(1).

[35] Regulation (EU) 2017/1128 of the European Parliament and of the Council of 14 June 2017 on cross-border portability of online content services in the internal market, OJ [2017] L 168/1.

[36] Regulation (EU) 2017/1128 of the European Parliament and of the Council of 14 June 2017 on cross-border portability of online content services in the internal market, OJ [2017] L 168/1, Article 8(2).

[37] On data licensing, cf. Kilian (2012), 169 and Joung et al. (2005). One should recognise, however, that "as any violation of data subject's personality rights are very context-sensitive, there remains a Damoclean threat to the validity of such contracts on data ('data licences') thus turning them into an imperilled high-risk transaction." (Sattler (2018)).

of September 2017,[38] finally, the European Commission recognised the principle of free movement of non-personal data. Correspondingly, they noted that obstacles to the free flow of data are in violation of the free movement of services and that data value chains are built on "data analysis, marketing, and distribution."[39]

Many perspectives will be left out of this paper, including the political campaign teams increasingly using the ability offered by social media platforms "to deliver targeted advertisements to selected lists of individual voters".[40]

The Article 29 Working Party[41] has clarified that the legal basis of processing for targeted advertising purposes is consent and that the only mechanism that is fully compliant with the then-effective Data Protection Directive[42] is a strong 'opt-in' one. Some judges[43] have followed this approach, thus considering illegal soft 'opt-in' mechanisms, such as a pre-ticked box that the user has to untick in order not to authorise data processing.

The *Vidal-Hall v. Google* case[44] has shown, on the one hand, how targeted advertising is an ideal prism to observe the intersection between data protection, competition, intellectual property, and consumer protection; on the other hand, it has spelt out the principle whereby it is not a requirement of data protection regimes that the loss be pecuniary; therefore, one can claim damages even for mere distress. This confirms that the nature of the interests involved in targeted advertising is not only financial, but also pertains to the user as a person. Moreover, *Vidal-Hall v Google* has confirmed that technological enforcement is not always sufficient. Indeed, in that case the users set Apple's Safari browser to block third-party cookies, but a Safari workaround operated by Google allowed it to record and use information about the users for the purposes of its advertising service.

Complicated algorithms are used by machines to get to know us better[45] and sell us what we desire (or sometimes what we do not even know we desire). However, one should not be inclined to (entirely) allocate the responsibility to autonomous artificial agents. As shown by the recent case of the Facebook 'trending list', where the human agents were selecting the posts to show in a non-neutral way, one cannot

[38] Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union, COM/2017/0495 final - 2017/0228 (COD).

[39] Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union, recital 2.

[40] European Commission (2016b), para. 3.4.4.

[41] Article 29 Working Party (2010). The Article 29 Working Party has been replaced by the European Data Protection Board (Article 68 of the General Data Protection Regulation).

[42] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ [1995] L 281/31.

[43] See, e.g., John Lewis v. Roddy Mansfield, unpublished, analysed by Groom (2014).

[44] Vidal-Hall & Ors v. Google Inc [2014] EWHC 13 (QB) (2014); Google Inc v. Vidal-Hall & Ors [2015] EWCA Civ 311 (2015). On 30 June 2016, Google withdrew its appeal from the Supreme Court. See, for instance, Evans (2015) 80; Chamberlain (2015) 93; Flint (2016) 38.

[45] Automated decisions do not always work. For instance, on 29 August 2016, Facebook blocked the accounts of many LGBT advocates because their posts had been judged … homophobic.

always blame an algorithm for the policies of these platforms. Therefore, a savvy framework for targeted advertising will strike a balance between the need to take into account the actual autonomy of artificial agents and the necessity not to let this act as an absolute disclaimer of human liability.

The structure of this paper is as follows. The starting point is the regulatory framework in Europe as clarified by the Article 29 Working Party and the European Data Protection Supervisor, with particular regard to the ePrivacy Directive.[46] Moving from the observation that actors in cyberspace tend (sometimes understandably) to ignore top-down regulations, since they prefer peer regulation, the International and European self-regulation initiatives of the International Chamber of Commerce (ICC), the European Advertising Standards Alliance (EASA), and the Interactive Advertising Bureau (IAB) will be critically analysed. A case study on Facebook and the use of data on sexual orientation is presented with regards to a hypothetical Italian user who lodges a complaint before the Istituto di Autodisciplina Pubblicitaria. This chapter goes on to compare the Data Protection Directive and the General Data Protection Regulation, with a focus on direct marketing, but touching also on profiling and algorithmic decision-making. Given that Google is the main actor in the targeted-advertising world, this chapter explains how the platform works and analyse, its terms, privacy policy (hereinafter 'legals') and settings options, to assess how data are treated with regard to this form of advertising. Before concluding, this work looks at targeted advertising from an intellectual property and competition law perspective. The chosen prism is the Facebook/WhatsApp concentration. The chapter aims to evaluate whether the decision of the Commission authorising the concentration would be different today, in light of the change to WhatsApp's privacy policy allowing the use by Facebook of certain data of WhatsApp's users. More generally, it is assessed whether targeted advertising can be prevented or somehow regulated through the unfair commercial practices regime. It is concluded with a pragmatic proposal which aims to empower the users, yet to strike a balance between their interests and rights and those of the businesses (ad networks, publishers, advertisers, etc.), i.e. the "Cooperative Charter on Online Behavioural Advertising." In general, the idea is that one should recognise that the opt-in regime required by some regulators is not implemented by the companies using targeted advertising; cumbersome regimes such as the notice and consent provided by the ePrivacy Directive have been a failure. Therefore, one should impose on businesses a more reasonable opt-out mechanism, providing that the right to dissent is actually enforced (as opposed to the current practice of circumventing adblockers and kindred tools) and that the information is clear, brief, and provided in an interactive and gamified way. The user has to be at the centre of the system, but it is debatable that data protection rules are the best means to ensure a user-centric system.

[46] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, or ePrivacy Directive), OJ [2002] L 201/37.

As to the methodology, alongside a review of legislations, regulations, self-regulations, legals, and literature in Europe (with a particular, albeit non-exclusive, focus on the UK and Italy), some experiments have been carried out with the aim of understanding: (1) How and how much are we tracked and, therefore, served with targeted advertising; (2) How effective are the technical tools a user can put in place to stop being the target of such advertising; (3) Whether users are aware they are tracked and whether they know what "targeted advertising" means". The sometimes-surprising results are presented below.

2 The European Regulation of Targeted Advertising

Data are commonly seen from the perspective of the data subject's rights to privacy and data protection, which have undoubtedly reached the status of fundamental human rights. However, phenomena such as targeted advertising shed light on the other face of data: users' data are becoming one of the most important assets in the IP portfolios of several businesses. Therefore, a balance has to be struck between competing interests.

Perhaps understandingly, the European regulators have favoured privacy and data protection over the other perspectives. The first—and currently most important—(quasi) regulation is the Article 29 Working Party's opinion on "online behavioural advertising" (OBA).[47]

Though the focus will be on the said opinion, some quick historical remarks are in order.

The relevant brief history might date back to 1993, when the Council of Europe's European Convention on Transfrontier Television[48] entered into force. However, at that time, given the development of the relevant technologies, targeted advertising was understood as advertising directed to audiences based in a single country. Indeed, under Article 16(1), in order to avoid distortions in competition and endangering the television system of a party to the Convention, "advertising and teleshopping which are specifically and with some frequency directed to audiences in a single Party other than the transmitting Party shall not circumvent the television advertising and tele-shopping rules in that particular Party".

Two years later an amendment was proposed to Council Directive 89/552/EEC on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities (Television Broadcasting Directive).[49] The Commission underlined that, in order to enable the broadcasting organisations and the national regulatory

[47] Article 29 Working Party (2010).

[48] The text is available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680007b0d8.

[49] See Commission of the European Communities (1995).

authorities to organise their activities efficiently, the Directive and the Convention should be as compatible as possible. It is noteworthy that as an example of fundamental difference between the two instruments reference is made to Article 16 of the Convention on targeted advertising that "has no equivalent in the Directive (given that it would be fundamentally incompatible with Article 59 of the Treaty)".[50] The reference seems to the Treaty of the European Economic Area that provided that "restrictions on the free supply of services within the Community shall be progressively abolished".[51]

A number of amendments have been introduced over the years and, ultimately, the Audiovisual Media Services Directive repealed the Television Broadcasting Directive.[52] One can infer from recitals 41 and 42 of the former that targeted advertising (understood as advertising directed to an audience in a country) is consistent with the EU law. Therefore, one has to believe that the Convention's rule on targeted advertising is no longer applicable in the countries which are parties both of the Council of Europe and of the European Union.[53] Indeed, Article 27(1) of the Convention states that in their relations with each other the Parties that are Members of the European Union will apply the latter's rules, and will apply the rules of the Convention only insofar as there is no EU measure relating to the particular subject in question.

Given that today one can watch television via the Internet (accessing it through multiple devices) and given the developments of smart TVs, as a policy recommendation one should wish that the Audiovisual Media Services Directive would soon be amended to take into account the possibility to serve advertisements targeted not only to an audience, but to a specific user. A new legislative proposal amending the said Directive was adopted by the European Commission on 25 May 2016, in the context of the Digital Single Market Strategy.[54] This proposal does not take into consideration our suggestion, which is surprising if one considers that television has the highest share of advertising revenue across all media,[55] therefore there is a significant interest in increasing targeted advertising through this channel.

A by far more up-to-date vision has been expressed by the Commission with regard to online platforms, even though the reference to targeted advertising is

[50] Ibid., para. 3.1.

[51] The original text of 1957 is available at: http://www.ab.gov.tr/files/ardb/evt/1_avrupa_birligi/1_3_antlasmalar/1_3_1_kurucu_antlasmalar/1957_treaty_establishing_eec.pdf.

[52] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive), OJ [2010] L95.

[53] For instance, Germany, Italy, and the UK. See the full list of signatories available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/132/signatures?p_auth=DyuOx8C9.

[54] Proposal for a Directive of the European Parliament and of the Council amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities, COM/2016/0287 final - 2016/0151 (COD).

[55] PwC (2015), as cited by the European Commission (2016d), para. 56.

arguably limited to the search engine platforms. It is noted, indeed, that some search engines use disaggregated data about users' online behaviour to provide targeted advertising.[56] The Commission points out that cookies should only be placed on a user's device after consent has been given. Taking a balanced (if not holistic) view, the Institution observes that "users encounter a dilemma in the face of a trade-off between ex-ante information benefits and ex-post risks".[57]

Coming to the cited opinion, according to the Article 29 Working Party, the first piece of legal framework one should take into consideration is the ePrivacy Directive. Under its Article 5(3),

> Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

Therefore, advertising network providers are allowed to place cookies or similar devices on users' terminal equipment or obtain information through such devices only with the informed consent of the users.

In order to review the ePrivacy Directive, the European Commission has launched a public consultation,[58] whose preliminary findings were published in August 2016.[59] There are two points that are particularly relevant for targeted advertising.

The first concerns cookies. According to 77% of citizens and civil society and 70% of public authorities, information service providers ought not to have the right to prevent access to their services if users refuse to have identifiers, such as cookies, stored in their terminal equipment. Three quarters of industry on the other hand disagree with this statement. As confirmed by the Google use case below, this is a hot issue. For instance, once one disables the cookies, one is no longer able to log in to Facebook. The social network platform does not explain why, but they say that cookies are necessary to access Facebook.[60] Twitter is somewhat clearer. It prevents users who disable cookies from accessing it, though it explains that Twitter and its

[56] European Commission (2016b), para. 3.3.4.7 refers to Eggers / Hamill / Ali (2013), 19.

[57] Ibid., with reference to Martens (2016).

[58] On 6 May 2015, the Commission adopted the Digital Single Market (DSM) Strategy, which announced that, following the adoption of the General Data Protection Regulation, the ePrivacy rules would also be reviewed. Therefore, on 11 April 2016, the European Commission launched a public consultation to seek stakeholders' views on the current text of the ePrivacy Directive as well as the possible changes to the existing legal framework to make sure it is up to date with the new challenges of the digital area. The consultation closed on 5 July 2016.

[59] European Commission (2016a). The full report can be found at https://ec.europa.eu/digital-single-market/en/news/full-report-public-consultation-eprivacy-directive.

[60] Consequently, this author could not access all the services he had registered with through the Facebook login, such as Spotify and Academia.edu.

partners use cookies for statistics, personalisation and advertising. To make a long story short, it seems that these tools the users theoretically have to prevent cookies and advertisements are more formal than substantial.

Another relevant issue in the preliminary report is the choice between opt-in and opt-out. Even though the question concerned marketing calls, the concept is the same, since targeted advertising is the premise for targeted marketing. All groups of respondents agree that Member States should not retain the possibility to choose between a prior consent (opt-in) and a right to object (opt-out) regime for direct marketing calls to citizens. Unsurprisingly, the stakeholder groups are split on which regime should apply: whereas close to 90% of citizens, civil society and public authorities favour an opt-in regime, 73% of industry favour an opt-out regime.

The consultation has partly informed the draft ePrivacy Regulation[61] that will change some relevant rules, such as the (no longer compulsory) cookies notice. In the version adopted by the Council in September 2017,[62] it presents a threefold strategy. Firstly, browser settings shall replace the cookie notice. Secondly, the exceptions to consent are clarified and expanded. Positively, the Presidency of the Council of the EU added a paragraph stating that the browser "shall provide in a clear manner easy ways for end-users to change the privacy setting consented to […] at any time during the use."[63] Thirdly, there is a (long overdue) shift from the right to consent to the right to withdraw. Particularly the first pillar is to be welcomed and it helps overcome the uncertainty as to whether browser settings could be deemed to deliver the user's informed consent or not.[64] If adopted, it would constitute also the partial overcoming of the European Parliament's position whereby OBA would constitute "a serious attack on the protection of privacy when it […] has not first been freely and explicitly consented to by the consumer".[65]

The Article 29 Working Party stresses that opt-out mechanisms do not in principle deliver data subjects' consent. Only in very specific, individual cases could implied consent be argued.[66] Therefore, the European data protection authority asks advertising network providers to create prior opt-in mechanisms requiring an affirmative action by the data subjects indicating their willingness to receive cookies or

[61] Commission, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications'), COM (2017) 10 final - 2017/03 (COD), 10 January 2017 (hereinafter draft ePrivacy Regulation).

[62] Presidency of the Council of the European Union, note n. 11995/17, 2017/0003 (COD), 8 September 2017.

[63] Ibid., Art. 10(2a).

[64] For this problem, related also to the opacity of privacy policies, see Commission, 'A comprehensive approach on personal data protection in the European Union' (communication) COM (2010) 609 final, para 2.1.5.

[65] European Parliament (n 15) para. I (see also ibid para 20).

[66] Different rules apply to sensitive data, e.g. health and sex data. Indeed, the only available legal ground for processing the data is explicit, separate prior opt-in consent (no opt-out, no browser settings).

similar devices and the subsequent monitoring of their surfing behaviour for the purposes of serving tailored advertising. Even though, to meet the requirements of Article 5(3) of the ePrivacy Directive, it is not necessary to request consent for each reading of the cookie, to keep data subjects aware of the monitoring, ad network providers should:

(i) limit in time the scope of the consent;
(ii) offer the possibility to revoke it easily; and
(iii) create visible tools to be displayed where the monitoring takes place.

It does not seem that these principles have been adopted by the main actors of the Web.

In the European regulator's view, "[b]ecause behavioural advertising is based on the use of identifiers that enable the creation of very detailed user profiles which, in most cases, will be deemed personal data, Directive 95/46/EC is also applicable".[67] The relevant obligations should be complied with not only by the ad network providers, but also by publishers. They can be both considered data controllers.[68] The Article 29 Working Party considers transparency as a key condition for individuals to be able to consent to the collection and processing of their personal data and exercise effective choice. However, what matters is not the information, but the actual possibility to dissent, which is usually denied.[69] Therefore, as a policy recommendation, one should go back to the version of Article 5(3) prior to the 2009 amendment[70] of the ePrivacy Directive. Indeed, the old provision recognised "the right to refuse such processing by the data controller".

There are two main ways of profiling users. One can distinguish between predictive profiles and explicit profiles. The former is created by observing individual and collective user behaviour over time, the latter from personal data that data subjects themselves provide to a web service. The privacy needs in the two scenarios are different. In the first one, indeed, users may not be aware of the fact they are being

[67] This is due, according to the Article 29 Working Party, to two reasons. On the one hand, behavioural advertising normally involves the collection of IP addresses and the processing of unique identifiers. On the other hand, the information collected in the context of behavioural advertising relates to a person's characteristics or behaviour and it is used to influence that particular person.

[68] As clarified by the Article 29 Working Party, the publisher's responsibility does not cover all the processing activities necessary to serve behavioural advertising, for example, the processing carried out by the ad network provider consisting of building profiles, which are then used to serve tailored advertising. However, the publishers' responsibility covers the first stage, i.e. the initial part of the data processing, namely the transfer of the IP address that takes place when individuals visit their websites.

[69] Cf. Hoofnagle et al. (2012), 273.

[70] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ [2009] L 337/11.

observed. Therefore, transparent and user-friendly information is critical. The role of this kind of profiling will increase exponentially given the developments of artificial intelligence and predictive analytics.[71] Consequently, one must remain particularly vigilant. In the second one, an anti-paternalistic approach should avoid imposing too heavy information burdens on the profilers. The free choice to give away certain data eases the data protection-related obligations, as long as the users are given the possibility to delete the account and/or the data any time and as long as the 'legals' are readable.[72] It is worth noting that the High Court of England and Wales in *Spreadex v Cochrane*[73] has clarified that the clauses of such never-ending legals are not binding for noncompliance with the unfair terms regime.[74]

The opinion of the Article 29 Working Party sets out the information obligations of advertising network providers/publishers vis-à-vis data subjects. In particular, an ad network provider who wishes to store or gain access to information stored in a user's terminal equipment is allowed to do so in two events. Firstly, if it has provided the user with clear and comprehensive information in accordance with GDPR, inter alia, about the purposes of the processing. Secondly, if it has obtained the user's consent to store or access information on the user's terminal equipment, after having provided the information requested.

The Article 29 Working Party goes on to reason that, based on the definition and requirements for valid consent ex Article 2(h) of Directive 95/46/EC, "data subjects cannot be deemed to have consented simply because they acquired/used a browser or other application which by default enables the collection and processing of their information". This seems to be confirmed by the GDPR. Under recital 32, indeed, "[s]ilence, pre-ticked boxes or inactivity should not […] constitute consent". Article 4(11) of the GDPR further provides that "'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". Arguably, methods such as that adopted by LinkedIn and Facebook, which equal using the site to agreeing to the cookie policy, are not compliant with the law.

The opinion further clarifies the obligations set forth by the applicable legal framework, by pointing out that for browsers' settings to be able to deliver informed consent, it should not be possible to circumvent the choice made by the user in setting the browser. We have already shown how the option to disable cookies is

[71] Cf. Neelam et al. (2015), 51; Kerr and Bornfreund (2005), 647.

[72] Noto La Diega (2016a) suggests a practical tool to overcome the opaqueness of the legals: the "awareness by design" app.

[73] Spreadex LTD v. Cochrane [2012] EWHC 1290. According to the court "[i]t would have come close to a miracle if [the defendant] had read" a specific sentence of a clause, "let alone appreciated its purport or implications, and it would have been quite irrational for the claimant to assume that he had" (Judgment at para. 19).

[74] The Court applied the Unfair Terms in Consumer Contracts Regulations 1999, which has now been substituted by the Consumer Rights Act 2015.

unworkable. Moreover, deleted cookies may be "respawned" by Flash cookies,[75] enabling the ad network provider to continue monitoring the user. New tracking vectors pop up constantly, for instance, HTML5 local storage and Cache Cookies via eTags. The latter is "capable of unique tracking even where all cookies are blocked by the user and 'Private Browsing Mode' is enabled".[76]

Finally, consent by browser setting to receive cookies in bulk is invalid, because it implies that users will accept future processing, possibly without any knowledge of the purposes or uses of the cookie.

Not long after the above analysed opinion, the European Data Protection Supervisor delivered a speech in the same vein, calling on the European Commission to ensure that Article 5(3) of the ePrivacy Directive is fully respected. The Supervisor pointed out that "systematic tracking and tracing of consumer behaviour online is a highly intrusive practice and is now rightly subject to more stringent requirements. Although initiatives for increased transparency and consumer control in the online environment are most welcome, this should not result in a limitation of consumer rights".[77] The statement criticises the European Commission for commending the EASA-IAB[78] Best Practice Recommendation[79] and Framework on behavioural advertising[80] and a US-driven 'do-not-track' initiative,[81] because they do not adopt the consent rule. This cast doubts (which then proved on this point baseless) on the position of the European Commission on this subject. The chapter, however, moves on to analyse the European and International self-regulation initiatives,[82] since they can affect businesses' and users' behaviour even more than regulations and hard law initiatives.[83]

---

[75] See Ayenson et al. (2011), 1.

[76] Ibid, 14. HTML5 may be used as well to enhance privacy.

[77] European Data Protection Supervisor (2011a). For the full speech, see Hustinx (2011).

[78] European Advertising Standards Alliance and Interactive Advertising Bureau.

[79] European Advertising Standards Alliance (2011).

[80] Interactive Advertising Bureau (2011).

[81] The reference is to the Network Advertising Initiative's (NAI) self-regulatory framework. In 2013, the NAI substituted the framework with a code of conduct update by NAI (2015a). Cf. also NAI (2015b) and Federal Trade Commission (2009). The US framework, which revolves around the concept of interest-based advertising, will not be analysed. It should be said, however, that, under the current regime (§II.C.1 of NAI (2015a)), companies should provide an opt-out mechanism for the collection and use of non-personally identifiable information for interest-based advertising purposes, whilst opt-in mechanisms are required for the use of sensitive data and precise location data.

[82] The national implementations of the said regulations will not be analysed. See, for example, Istituto di Autodisciplina Pubblicitaria (IAP) (2015), for the Italian regulation. Complaints can be filed online with the Comitato di Controllo IAP, which double-checks compliance with the EASA/IAB self-regulations. If necessary, the IAP applies the EASA Cross Border Complaints system.

[83] Given that the Internet operates outside a precise physical location it is hard to enforce the laws and it is often unclear which national or regional institution should govern and regulate the relevant activities. Therefore, self-regulatory initiative, by being independent from geographical boundaries and by virtue of peer-pressure mechanisms, can be more effective.

3 European and International Self-Regulation of Targeted Advertising

In Europe, the public debate on OBA started as a spin-off of the general debate on the 2009 amendment to the ePrivacy Directive. In 2010, then Digital Agenda Commissioner Neelie Kroes challenged the advertising industry to provide the European citizens with greater empowerment through transparency, consent, user-friendliness, and effective enforcement.[84] In a wise speech, the Commissioner underlined that one has to strike a balance between protection of personal data and enabling innovation in advertising and that "privacy regulation does not exist in a values vacuum".[85] Therefore, one has to take into account the effects of the regulation on industry and its practicality, and "to consider the long-term health of digital environments".[86] Hence, she called for a self-regulatory solution, with the caveat that "it will need to be one clearly based on the applicable EU legislation". The below assessment shows that the opt-out approach taken by the industry does not entirely comply with the European legal framework, even though some good steps have been taken.

The IAB is a global non-profit group open to companies engaged in the sale of interactive advertising and marketing. In April 2011, the group developed a European self-regulatory framework for OBA (henceforth "the Framework"). The Framework lays down a structure for codifying industry good practices and establishes some principles to increase transparency and choice for web users within the EU/EEA which are binding upon the companies and associations that are part of IAB.

The pillars of the Framework are notice, user choice, data security, sensitive segmentation, education, compliance and enforcement, and review. These principles apply consumer-friendly standards to OBA and the collection of online data in order to facilitate the delivery of advertising based on the preferences or interests of web users.[87]

The second principle regards the user choice over OBA. Explicit consent is required only when a company collects and uses "data via specific technologies or practices that are intended to harvest data from all or substantially all URLs traversed by a particular computer or device across multiple web domains and use such data for OBA" (II.B).[88] Explicit consent is required as well if one seeks "to create or

[84] It should be noted that EASA interprets Kroes's pillars differently, referring to them as "transparency, choice and control" (available at: http://www.easa-alliance.org/issues/oba).

[85] Kroes (2010).

[86] Ibid.

[87] The regulation of the content of online advertisements and the advertisement delivery are out of the scope of the Framework.

[88] Under principle II.C of the Framework, then, companies "that have obtained Explicit Consent pursuant to II.B should provide an easy to use mechanism for web users to withdraw their Explicit Consent to the collection and use of such data for OBA".

use such OBA segments relying on use of sensitive personal data" (IV.B). As to the other scenarios, third parties "should make available a mechanism for web users to exercise their choice with respect to the collection and use of data for OBA purposes and the transfer of such data to Third Parties for OBA" (II.A).

Such choice should be made available in two ways. Firstly, third parties "should give clear and comprehensible notice on their web sites describing their Online Behavioural Advertising data collection and use practices" (I.A.1).[89] Secondly, they should refer to the YourOnlineChoice.eu website (also "OBA User Choice Site").

On 19 August 2016 at 10:43 GMT, this author visited the site and went to the "Your Ad Choice" section, where a message popped up: "Your Chrome browser blocks cookies used for behavioural advertising purposes. To successfully switch off behavioural advertising these cookies need to be enabled". Therefore, strangely enough, one has to enable OBA cookies to disable targeted advertising. The system double-checked this author's status with regard to 119 companies. In this occasion, it was found that three companies this author had never heard of before (Delta Projects, Captify, Atlas Solution) were delivering him targeted advertisements, even though he had always blocked third-party cookies and he had installed AdBlock Plus. Moreover, no company displayed the icon indicating that the "company is not delivering advertisements customised to your interests".[90]

It is commendable that the site adopts a user-friendly icon (see Fig. 1) that contains a hyperlink to the OBA User Choice Site or to the third party notice. It can be used to turn off OBA by some or all companies.

However, the said site is not very clear, since it does not show the user's status with regard to most of the companies and the majority of the displayed companies

Fig. 1 Online behavioural advertising icon

[89] The notice should include: (a) The identity and contact details of the third party; (b) The types of data collected and used for the purpose of providing OBA, including an indication of whether any data is "personal data" or "sensitive personal data"; (c) The purposes for which OBA data are processed and the recipients to whom such data might be disclosed; (d) An easy-to-use mechanism for exercising choice with regard to the collection and use of the data for OBA purposes and to the transfer of such data to Third Parties for OBA; (e) The statement that the company adheres to these principles; and (f) A link to www.youronlinechoices.eu, a consumer-focussed website and education portal.

[90] 28 companies were "experiencing technical issues, and […] cannot retrieve your status" (Google and Facebook were among them), and 18 companies had "not set-up a cookie, but may deliver in the future advertisements that are customised to your interests". No results were displayed for the remaining 60 companies.

were encountering technical issues, thus impeding the retrieval of the status.[91] Moreover, it is not easy to assess the reliability of the tool. The experiment was repeated on 20 August 2016 at 10:28 GTM and results regarding only 8 companies (as opposed to 49) were displayed. This time the only company that was targeting this author was Accordant Media, 4 companies were experiencing technical issues and 3 companies had not set up a cookie, but might in the future deliver advertisements customised to his interests. Finally, the experiment was repeated a third time on the same day at 10:45 GTM and the results were again different. This time, this author was offered targeted advertising by ADEX, results regarding 18 companies were displayed, 3 companies had not set up a cookie, but might in the future deliver advertisements customised to his interests and 14 were experiencing technical issues. Accordant Media was one of the companies encountering technical issues, and thus not able to retrieve the relevant status.

The IAB's framework, based on an opt-out mechanism with minor exceptions, is complemented by the EASA Best Practice Recommendation on OBA (hereinafter "the Recommendation"). EASA is a non-profit organisation dealing with advertising self-regulation issues and bringing together 34 national advertising self-regulatory organisations and 16 organisations representing the advertising industry.

The Recommendation provides "a pan-European, industry-wide self-regulatory standard for OBA, which empowers consumers across Europe".[92]

It recommends the industry members to (a) Clearly support the adoption at local level of rules on OBA based on the Recommendation; (b) Clearly support the adoption at local level of the new remit and rules for the handling of complaints on OBA by self-regulatory organisations; (c) Establish a clear agreement with the ad networks regarding the handling of complaints of a non-technical nature by the advertising self-regulatory bodies; (d) Ensure adequate industry and consumer awareness of the above; (e) Ensure the necessary linkup with the consumer controls page to create a one stop shop for consumer feedback and complaints; (f) Ensure the necessary linkages between industry compliance monitoring reports and the complaint handling processes; (g) Establish robust measures for sanctions related to repeat offenders or rogue traders.

The Recommendation draws its principles from those of the IAB Framework; however, it leaves out data security and education. EASA adopts the same opt-out mechanism with limited exceptions proposed by IAB, with the (unnecessary?) precision that when "a web user exercises his/her choice and objects to OBA data collection, OBA processes should no longer be used by that entity to facilitate the delivery of targeted online advertising to that user's browser".[93]

Probably the most interesting part of the Recommendation regards enforcement: "[a] consumer could be making his feedback/complaint either directly to a company, to a Third Party or Website Operator, a regulatory authority, a self-regulatory

[91] This author tried to retrieve his status with regards to Google until 16:43 GMT of the same day.

[92] http://www.easa-alliance.org/issues/oba.

[93] European Advertising Standards Alliance (2011), Principle II.A.

body or a similar local alternative dispute resolution (ADR) body (e.g. a consumers association). These would form different routes which could all transit a one stop shop for compliance. This would consist of a web page where the transfer of feedback/complaints would be passed to the relevant process and organisations."[94] One has to distinguish two scenarios. On the one hand, consumer feedback regarding technical issues on OBA (e.g. about who is serving OBA) would be handled by an industry web-based interface. On the other hand, consumer complaints arising from dissatisfaction with the way their initial feedback or complaint have been handled via the industry interface or complaints about more general privacy issues or issues related to the content of advertising would be handled by a process involving the advertising self-regulatory bodies.

The procedure in the second scenario is as follows. The scenario regards the use of a user's sexual orientation data for OBA purposes without that user's explicit consent. On 20 August 2016 at 12:30, this author conducted an experiment to assess whether sensitive data about sexual orientation were exploited to serve targeted advertisements or not. Therefore, he googled "gay.com", "gay dates", and "Grindr" (a popular gay dating mobile app). He then refreshed his Facebook feed and nothing gay-related appeared for some time. At 14:45 GTM, Facebook suggested him to subscribe to a group for "Sicilian gay bears". However, this cannot be considered advertising, because the group was not selling products or services. At the same time, scrolling down the page this author noticed the sponsored page "Meetic.it", which showed pictures of women. One might infer, hence, that Google and Facebook are not (directly) exploiting sensitive data on sexual orientation, but they might deduce from search terms that the user is looking for dates and the like. The experiment should be repeated and the results observed for a longer period, in order to present a more reliable outcome. For instance, it may not necessarily be a coincidence that, on the same day at 21:22 GMT, when this author was accessing Facebook via his smartphone, he was shown the advertisement of "Mrb&b", an app (and service) for people looking for temporary gay-friendly accommodations. Likewise, the day after, at 00:02, he was shown an advertisement of the Western Fertility Institute, which provides surrogacy services to same-sex couples.

If one were convinced that Facebook[95] was exploiting data on their sexual orientation without one's explicit consent (or for other non-technical reasons), one should

[94] Ibid., 27.

[95] Practically, if this author represented as legal counsel a customer wanting to file a complaint in this case, pragmatically he would file it against both Facebook Ireland Limited and SFO84, Inc. (the owner of Mrb&b). However, it is plausible that the real defendant be the former, since it has the control over its users' data. If one reads European Commission, Case No. M.7217 – Facebook/WhatsApp, 3 October 2014, para 70, on the Facebook – WhatsApp merger, they will notice that, for the purpose of its online advertising activities, "Facebook collects data regarding the users of its social networking platform and analyses them in order to serve advertisements on behalf of advertisers, which are as much as possible "targeted" at each particular user of its social networking platform. However, Facebook does neither sell any of the user data it collects nor provides data analytics services to advertisers or other third parties as a stand-alone product separate from the advertising space itself". This means that SFO84, Inc. does not have access to Facebook users' data and, therefore, it could not be considered liable for any illegal use of them.

proceed as follows. One should turn to one's national self-regulation authority or organisation, for instance the Istituto di Autodisciplina Pubblicitaria (IAP) in Italy.[96] The IAP would assess whether it is competent in the matter or needs to transfer the complaint to the competent self-regulation authority following the EASA Cross-Border Complaint rules[97] (for instance, it could transfer it to the Deutsche Datenschutzrat Online-Werbung or to the Advertising Standards Authority in the UK).[98] If it is competent, the IAP will then decide whether the complaint is of substance.[99] In particular, if the complaint does not raise any issue under the IAB Recommendation, it will inform the user that their complaint cannot be handled. If it deems that the complaint should be pursued, the IAP will contact the company concerned (in this case, Facebook) or refer the complainant to the latter. At this point, Facebook would be given the opportunity to resolve the issue informally, with or without mediation by the IAP, which should be informed of the outcome. If Facebook refused to resolve the complaint, did not resolve it satisfactorily or did not react to the enquiries, the IAP would launch a formal investigation. The IAP may consult experts in order to decide whether the company has breached the rules. The IAP's jury (the Comitato di Controllo, which may refer to the Giurì),[100] subsequently, would adjudicate the complaint. The ruling would be communicated to the parties (the main decision being the *ingiunzione di desistenza* to make the company desist) and then published on the website of the IAP and its database, with the names of the parties listed. If Facebook did not comply with the ruling, the jury would reiterate the *ingiunzione di desistenza* and would have it published in the newspaper, with the costs covered by Facebook itself. Should it continue to breach the rules on a persistent and deliberate basis, the IAP would apply other sanctions such as industry or relevant statutory referral.[101]

[96] The form to fill in is available at: http://www.iap.it/le-attivita/per-i-cittadini/pubblicita-comportamentale-online/.

[97] Reviewing European Advertising Standards Alliance (2015a), one can notice that 100% of the reported complaints falling under the category "privacy and data protection" are about OBA. The other categories are misleading advertising, social responsibility, taste and decency. Of the 26 total complaints, six were about "privacy and data protection", and hence about OBA. Therefore, OBA complaints amount to more than 23% of the total.

[98] One has to look at the country where the medium carrying the advertisement is based; in the case of direct mail and digital marketing communications, the country where the advertiser is based; and in the case of OBA, the country where the principal decision-maker is established. See European Advertising Standards Alliance (2014), II.

[99] The self-regulation authorities and organisations (and this is the case with the IAP) usually invite the user to contact directly the interested company before filing a complaint.

[100] The Comitato di Controllo can refer to the Giurì cases of noncompliance with the Codice di Autodisciplina della Comunicazione Commerciale (Advertising Self-Regulation Code, updated on 22 March 2016). It can exert moral suasion, by inviting the advertising companies to edit the advertisement or the accompanying information. It can also issue injunctions to oblige the company to desist and to comply with the Codice (ingiunzione di desistenza). Injunctions can be issued by the Giurì as well, should the Comitato refer to it or should an *istanza* be filed. The user can complain informally to the Comitato (*segnalazione*) and formally to the Giurì (*istanza*).

[101] Industry referral would lead to other sanctions, such as loss of the right to use the B2B seal.

Given the growing importance of non-European advertising companies, one should have a look at the international self-regulation of advertising. The EASA has contributed to the revision process of the ICC Code on Advertising and Marketing Communication Practice.[102] It is interesting that, when commenting on the most significant changes to the Code, the first example given by the ICC is that "[f]or the first time the Code addresses responsibility with respect to the use of online behavioural targeting in the delivery of advertisements". Indeed, now art. D7 regulates "Provisions for online behavioural advertising (OBA)", in a way which is unsurprisingly very similar to that of IAB and EASA. Limiting the focus to the notice mechanism, it is provided that third parties and website operators should give "clear and conspicuous notice on their websites describing their OBA data collection and use practices".[103] It is not commendable that "notice should be provided through deployment of *one or multiple* mechanisms for clearly disclosing and informing Internet users about data collection and use practices".[104] This could lead to an overload of information. Explicit consent is limited to "[t]hose collecting and using data via specific technologies or practices that are intended to harvest data from all or substantially all websites traversed by a particular computer or device across multiple web domains, and use such data for OBA".[105] Two provisions of the Code deserve a particular mention. First and more importantly, under art. D8, "[a]nyone taking part in the planning, creation or execution of digital marketing communications including OBA, has a degree of responsibility […] for ensuring the observance of the Code towards those affected, or likely to be affected". This provision is flexible enough to fit the intricate supply chain of advertising (with responsibilities mainly shared between ad networks, advertisers, and publishers). Second, "[t]ransparency of data information collection and use, and the ability for users and consumers to choose whether to share their data for OBA purposes is vital".[106]

The international and European self-regulation systems are based on an opt-out mechanism which does not seem consistent with the law, in particular with the ePrivacy Directive[107] and with the GDPR. What is worse, the analysed self-regulation initiatives "create the wrong presumption that it is possible to choose not be tracked while surfing the Web".[108] Moreover, the opt-out tools can be and are sometimes ineffective. For instance, as one can read in the last report[109] on cross-border

[102] International Chamber of Commerce (2011).

[103] Art. D7.1 of the ICC Code of Conduct.

[104] Ibid., italics added.

[105] Art. D7.2 of the ICC Code of Conduct.

[106] Art. D7 of the ICC Code of Conduct.

[107] This is the main conclusion of Article 29 Working Party (2011).

[108] Ibid.

[109] In the previous report, European Advertising Standards Alliance (2015b), the only case about OBA regards the opt-out mechanism, because the user "had continually been unable to opt out of OBA data collection and use". The Autorité de Régulation Professionnelle de la Publicité resolved the complaint informally.

complaints,[110] in all the cases regarding OBA, the users complained about the opt-out mechanism because "they had continually been unable to opt out of OBA data collection and use"[111] or "[d]espite selecting the 'Off' mode, the website kept on reverting to 'On' mode".[112] As already said, even if the right to consent is critical, one should start by ensuring the right to dissent, because in its present unenforced form it has no real effect. Furthermore, even though there seems to be an increasing percentage of users clicking on the OBA icon,[113] there is no evidence that users actually know and understand what OBA is. On the contrary, this author has conducted a small-scale poll on Facebook. Its outcome is that 46 users did not know what targeted advertising was, whereas 10 users knew (one of which was an advertiser herself) and one was undecided. Notwithstanding the scale of the observation, a percentage of 17.5% has to be considered worryingly low, especially considering that the target users were young and highly educated.[114]

4 Profiling, Direct Marketing and Algorithmic Decision-Making in the General Data Protection Regulation

In 2013, a Member of the European Parliament asked the Commission if, in connection with targeted advertising, they could explain "why Facebook says it does not search for data, via keywords for example, in private and not public emails, but appears to be doing so anyway".[115] This is a common practice. For instance, on 20 August 2016 at 11:50 GTM this author accessed his Gmail account and he was shown an advertisement on the "MIT Big Data Course". After clicking to learn more details, he was informed that he had been targeted due to the content of his emails and on the basis of the information of his Google account.

The Commission replied that the then proposal for a GDPR "clarifies and strengthens the rights of data subjects in the context of online activities, such as social networking: providers must take account of the principle of 'data protection

[110] European Advertising Standards Alliance (2015a).

[111] 2914-5 Rubicon Project; 2916-7 Audience Science; 2922-3 Xaxis, 2920-1 Infectious Media, 2918-9 Captify. The Advertising Standards Authority upheld the complaints.

[112] 2969 Eyeota Ltd. The Deutsche Datenschutzrat Online-Werbung decided that the problem lay with the complainant: their technical device, privacy setting or Internet connection.

[113] 1 in 4 surveyed users in European Interactive Digital Advertising Alliance and TRUSTe (2015) have engaged with the OBA icon.

[114] A one-day survey of some of this author's Facebook friends was conducted on 21 August 2016. Their age range was 18-40 with a majority of people in their early thirties. Apart from the 18-year-old user and a user who did not attend any university, the rest of them had (at least) a master's degree (20 of which with a law background), whilst 7 users had completed a Ph.D. (two of them were professors).

[115] Tarabella (2013).

by default'".[116] It further pointed out that "[c]ompanies will be obliged to inform individuals as clearly, understandably and transparently as possible about how their personal data will be used, so that they are in the best position to decide what data they share".[117]

Strictly speaking, this reply did not really address the issues related to targeted advertising. Therefore, it can be useful to have a closer look at the Regulation to assess whether the problem has been taken into specific consideration.

The review process of the Data Protection Directive started in 2009[118] and the first driver determining the environment in which the review process took place was technological development. Indeed, "[t]echnological phenomena like cloud computing, behavioural advertising, social networks, road toll collecting and geolocation devices profoundly changed the way in which data are processed and pose enormous challenges for data protection".[119] Therefore, the European Data Protection Supervisor suggested the insertion of a "specific provision protecting children against behavioural advertising".[120] Even at that time it was clear that the problem was not merely about the provisions themselves, but mostly about their enforcement. When stressing that there were areas where "full compliance needs to be monitored and enforced",[121] the Supervisor referred specifically to the proceeding of the Commission against the UK for alleged breach of various data protection provisions, including the requirement of confidentiality of electronic communications in respect of behavioural advertising.[122]

---

[116] Reding (2013).

[117] Ibid.

[118] For a history of the law-making process see de Hert / Papakonstantinou (2016), 181.

[119] European Data Protection Supervisor (2011b), para 14. This opinion elaborated on Article 29 Working Party and Working Party on Police and Justice (2009), a milestone in the review process that led to the adoption of the General Data Protection Regulation. However, the contribution was limited to the observation that, "in specific cases, specific legislative measures embedding the concept of 'privacy by design'" (para 56) should be adopted. This was deemed to be the case with RFID technology, social networks, and behavioural advertising. It was also said that, given that the duty to inform the data subject is not always properly put into practice, a new legal framework should provide alternative solutions, in order to enhance transparency. For instance, "new ways to inform data subjects could be developed in relation to behavioural advertising" (para 63).

[120] Ibid., para 94.

[121] Ibid., para 162.

[122] The reference is to the "Phorm" case. The Commission launched legal action against the UK on 14 April 2009; the case entered its second phase on 29 October 2009. On 30 September 2010, the European Commission decided to refer the UK to the Court of Justice, but the former decided to close the case after the UK amended its national legislation so as not to allow interception of users' electronic communications without their explicit consent, and established an additional sanction and supervisory mechanism to deal with breaches of confidentiality in electronic communications. In particular, the Regulation of Investigatory Powers Act 2000 (RIPA) was amended to remove references to implied consent and to establish a new sanction against unlawful interception, which previously fell outside the scope of RIPA. On the Phorm case see Bernal (2012); Bray / Griffiths (2008), 24; Linkomies (2008), 12; Graham / Anderson (2008), 10.

This position has its roots in an opinion of 2010, when the Supervisor clarified the importance of privacy by default browser settings to guarantee informed consent to receive advertisements. It was noted, indeed, that "in practice very few people exercise the opt-out option, not because they have made an informed decision to accept behavioural advertisement, but rather because they do not realise that by not using the opt out, they are in fact accepting".[123] The interpretation of the existing rules was not deemed to be sufficient. Mandatory privacy by default settings are indicated as the solution whereby the users will have to change the browser settings if they are willing to receive targeted advertisements. In particular, it was held that the browsers should be set to reject third party cookies by default and new legislation should "require users to go through a privacy wizard when they first install or update the browser".[124]

After much debate, the European Commission published its proposal for a GDPR,[125] which differed from the versions of the Parliament[126] and the Council,[127] and all the more from the final instrument, adopted on 27 April 2016, which will apply from 25 May 2018.

It is noteworthy that the Economic and Social Committee, in opining on the Commission's proposal, stressed that one of the things to be included in the scope of the regulation should have been search engines, "the majority of whose revenue comes from targeted advertising thanks to their collection of personal data concerning the visitors to their sites, or indeed the profiling of those visitors".[128]

Now, under art. 14(1) of the Data Protection Directive, Member States shall grant the data subject the right "to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses". Given that targeted advertising is usually based on predictive analytics and algorithmic decisions, art. 15 ("Automated individual decisions")

[123] European Data Protection Supervisor (2010), para 96.

[124] Ibid., § 116(c).

[125] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 11 final — 2012/011 (COD).

[126] European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 - C7-0025/2012 - 2012/0011(COD)).

[127] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Preparation of a general approach, 9565/15.

[128] Opinion of the European Economic and Social Committee on the 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)' COM (2012) 11 final — 2012/011 (COD), § 1.10.

applies as well. Under its first paragraph, "Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc." This provision is particularly relevant, because it is not limited to direct marketing (targeted advertising may be considered as different from, albeit intrinsically connected with, direct marketing) and because thanks to its generic reference to automated decisions affecting (not necessarily from a pecuniary point of view) the user, it fits targeted advertising scenarios well.

Nothing in this provision expressly mentions advertising, even though the same rules should apply to the processing carried out for both the purposes, since they are intrinsically connected and sometimes hardly distinguishable. Nonetheless, one has to appreciate that at least the GDPR mentions online advertising. Its recital 58 stresses the importance, in order to comply with the transparency principle, that the information is concise, easily accessible, easy to understand, clear, in plain language and, where appropriate, accompanied by visualisation. Transparency is deemed to be "of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising".

Going on to the substantive law, the regulation of the right to object is not radically different from that of the Data Protection Directive. Indeed, under art. 21(2) GDPR, "[w]here personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing". On the one hand, some elements seem to lower the user's protection. For instance, there is no longer reference to the fact that the exercise of the right to object should be free of charge[129] and that the data subject should be informed before personal data are disclosed to third parties or used on their behalf for the purposes of direct marketing. Moreover, no mention is made of the duty to ensure the users' awareness of the right to object. On the other hand, commendably, there are at least four elements which constitute evidence of an increased protection. Firstly, and most importantly, there is a shift from a subjective approach to an objective one. Under the Directive, what mattered was the marketing purpose as anticipated by the controller. Under the GDPR, in turn, what matters is the marketing purpose per se, thus not allowing defences whereby controllers assert that they did not anticipate the use of the data for marketing purposes. Secondly, profiling is now expressly covered by the right to object (no reference whatsoever to profiling was contained in the Directive). Thirdly, under art. 21(3), "[w]here the data subject objects to processing for direct marketing purposes, the personal data shall

[129] However, national lawmakers, regulators and judges may clarify this aspect. For instance, Information Commissioner's Office (2016), 23, points out that "You must deal with an objection to processing for direct marketing at any time and free of charge".

no longer be processed for such purposes". From a policy point of view, it is a very peculiar provision. Indeed, if the data subject has the right to object to the processing of his or her data for direct marketing purposes, it is in the very nature of things that further processing for marketing purposes would be illegal. Therefore, the provision has two possible interpretations: either it is the sign of the lawmaker's awareness of the commonplace circumvention of anti-tracking tools, or it is a backdoor for the controllers to retain the data and use them for other purposes. In this case, they could keep using the data, without the user's consent, for purposes "compatible with the purpose for which the personal data are initially collected".[130] Fourthly, whereas under the Directive the right to object could be exercised "on request", now the data subject "may exercise his or her right to object by automated means using technical specifications",[131] a sort of objection by design (e.g. through adblockers). Even though that "may" weakens the provision, it may still constitute an element adblocking companies could use against companies purporting to circumvent adblockers.

There are other unclear provisions. For instance, the right to object to direct marketing should be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information" (art. 21(4)). This risks becoming a classic case of overload of information. For instance, should every website present the user with, say, separate notices for cookies and direct marketing? It shall be seen if the revision of the ePrivacy directive takes account of these issues.[132]

Furthermore, it is questionable whether the new provision on automated individual decision-making constitutes a step forward. Indeed, under art. 22(1) GDPR, the "data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her". This "similarly" may narrow the scope of the provision, as compared with the previous wording. However, two innovations are to be commended. Firstly, in principle automated decisions cannot be taken on the basis of sensitive personal data. Secondly, even in the cases when the right not to be subject to automated decision-making does not apply, now the "data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision". This is a victory for those who think that human decision-making can still be better than its automated counterpart.

A target of specific interest for the European legislature are children. Indeed, under recital 38, "specific protection should […] apply to the use of personal data of

[130] See art. 6(4) GDPR on the scenarios where processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent.

[131] GDPR, Article 21(5).

[132] According to European Commission (2016b), 3.5.5.2, following the adoption of the GDPR, "which includes provision regarding the right of individuals to object, including to direct marketing, there is a review of the ePrivacy directive, which must be in line with the new data protection rules".

children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child". But how is this specific protection structured? Where the child is below the age of 16 years, "such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child" (art. 8(1)). It is hardly imaginable that a 15-year-old guy would call his parents and ask for their authorisation every time Facebook or Google are processing his data. However, what strikes is not this rather ludicrous provision. It is that, under art. 8(2), the controller "shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology". This might be used to justify the use of biometrics (such as face recognition, gait recognition, etc.) to verify the age of the user.[133] The remedy risks being worse than the disease.

As observed by the European Commission, what matters is not (necessarily) the right to consent, but the right to dissent. Indeed, the last new provision that deserves to be stressed is that now direct marketing is a 'legitimate interest' to process the users' personal data without their consent (recital 47).[134] This may be interpreted as the result of a balance between data protection and freedom of enterprise. Indeed, competitiveness may be hampered if an undertaking is required to obtain the users' consent prior to any processing for targeted advertising and direct marketing.

More generally, there are provisions which do not directly focus on direct marketing, but will affect it nonetheless.[135] For instance, the GDPR, unlike the Directive, will apply to the processing carried out even by a controller or processor not established in the Union of personal data of subjects who are in the Union, whenever (1) the processing activities are related to either the offering of goods or services, irrespective of whether a payment by the data subject is required, and (2) the processing

[133] See, for instance, BioPay biometric payments system to verify the age of customers of retail shops. According to Woodward (2000), however, "there are no age verification biometrics".

[134] The "legitimate interest" justification for processing cannot be used, however, to violate the data subject's fundamental rights, including data protection and privacy. Indeed, the legitimate interest goes with the proviso that "the interests or the fundamental rights and freedoms of the data subject are not overriding" (recital 47, see also art. 6(1)f). On data protection and privacy as fundamental rights see, for instance, arts. 7-8 of the Charter of Fundamental Rights of the European Union, Article 16(1) TFEU, art. 8 ECHR, art. 1(2) GDPR, art. 1(1) Data Protection Directive. In the case law, ECJ, Case C-553/07, *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer*, 7 May 2009, ECLI:EU:C:2009:293, para. 47; ECJ, Case C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others,* 8 April 2014, ECLI:EU:C:2014:238, para. 53. As reminded, for instance, in ECJ, Case C-362/14, *Maximillian Schrems v Data Protection Commissioner,* 6 October 2015, ECLI:EU:C:2015:650 para. 38 "the provisions of Directive 95/46, inasmuch as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to respect for private life, must necessarily be interpreted in the light of the fundamental rights guaranteed by the Charter".

[135] On some other aspects see Bauer / Eickmeier (2016).

activities relate to the monitoring of their behaviour as far as their behaviour takes place within the Union.[136]

Overall, then the GDPR constitutes increased protection of the data subject, with some flaws. Alongside what is said above, for instance, it is submitted that referring to targeted advertising instead of direct marketing would have been preferable. For instance, it seems rather unfair that citizens can prevent companies from selling them products, but cannot avoid targeted advertising aimed to influence their voting preferences. Much will depend on how the courts will interpret the GDPR.

5 "It's a Google Market": Adsense, a Recent Change to the Google Privacy Policy and Related Details

Advertising "is a Google market"[137] and Google-controlled cookies are present on 97 of the top 100 sites.[138] In 2015, Google's ad revenue amounted to more than USD 67 billion, thus accounting for the majority of the online company's total revenues.[139] Its position in the advertising market is growing steadily.[140]

Many users have been surprised to find out that Google records and stores their voice and that they can listen to it.[141] Google tracks and profiles users across all their devices (which is worrying in an Internet of Things environment),[142] using the data collected by its services (e.g. Search, YouTube, Maps) and storing all their searches, browsing history, and locations, thus enabling Google and its partners to have the full picture of who a user is and what he desires.

The search engine service plays a critical role in enabling Google to take the leading position in the targeted advertising market. Indeed, as called to mind by the Commission in the working document accompanying its recent communication on

[136] European Commission (2016c), 148-149.

[137] This was the statement of Ernie Cormier, then president and CEO of Nexage, to Rowinski (2011). In the meantime, Nexage has been acquired by Millennial Media for USD 108 million. Millennial Media has recently been bought by AOL for USD 238 million.

[138] Ayenson et al. (2011), 1.

[139] See the summary of the relevant statistics, available at: http://www.statista.com/statistics/266249/advertising-revenue-of-google/.

[140] Comparing 2015 and 2016, there has been an increase of 18% (https://abc.xyz/investor/news/earnings/2016/Q3_alphabet_earnings/).

[141] This author has listened to his own recorded voice by visiting https://myactivity.google.com/myactivity?restrict=vaa&utm_source=help and it is noteworthy that Google recorded his voice several times without him having actually uttered the words "OK Google".

[142] On the one hand, the interaction between the devices creates highly valuable and potentially personal big data; on the other hand, the devices are increasingly equipped with sensors capable of collecting new types of data. This is confirmed by Google's Advertising page (https://www.google.it/intl/en-GB/policies/technologies/ads/): "[w]e may also select advertising based on information about your computer or device, such as your device model, browser type or sensors in your device like the accelerometer".

online platforms,[143] Google is the most frequently used search engine in most EU countries, where it handles about 90% of search queries. It is unlikely, moreover, that the situation will change, due to the fact that significant costs are involved in creating a web index, developing a search algorithm and building computing centres.[144] Therefore, cost-related economies of scope and scale allow search engine providers (primarily Google) to extract precious information from the large amounts of historical data from search queries submitted by users as well as other types of activity conducted by the users of the platform (email, use of maps, video, operating systems, internet browsers) and "[t]his argument is applicable for targeted advertising as well".[145] One needs only remember that the Court of Justice was able to condemn Google in the *Google Spain* case only because it found that advertising and search were "inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine at issue economically profitable and that engine is, at the same time, the means enabling those activities to be performed".[146]

Google shows ads based on:

i. The types of website that the user visits and the mobile apps that they have on their devices;
ii. Cookies on the user's browser and the settings in the Google account;
iii. Websites and apps that the user has visited that belong to businesses that advertise with Google;
iv. The user's activity on another device;
v. The previous interactions with Google's ads or advertising services;
vi. The user's Google account activity and information.[147]

From the ad settings page,[148] one may get the impression that the system is an opt-in one. Indeed, Google informs you about targeted advertising and it gives you the option to agree or not. Looking closer, however, one reads that "the Ads Personalisation setting *currently allows* Google to use data in your account to tailor ads that appear in Google products [and] on websites and apps that partner with Google" (emphasis added). This means that even if you do not express any consent, you will be served with bespoken advertisements. The legality of an opt-out mechanism for targeted advertising is indeed debatable.[149]

[143] European Commission (2016b).

[144] In 2014, for instance, Google spent approximately USD 11 billion on real estate purchases, production equipment, and data centre construction and USD 10.5 billion on R&D.

[145] European Commission (2016b), § 3.3.3.1.

[146] ECJ, Case C-131/12*, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, date of the judgment, ECLI:EU:C:2014:317, para. 56.

[147] About Google Ads, available at: https://support.google.com/adsense/troubleshooter/1631343.

[148] https://www.google.com/settings/u/0/ads/authenticated.

[149] This cannot be inferred from the ads setting page, but it can be from the bottom of the DoubleClick cookies page. More transparency would be preferable.

The users are offered some tools to delete the personal information regarding them and, sometimes, to prevent its collection.[150] However, these means are not always user-friendly and, what is more important, they can be circumvented, as the *Vidal-Hall v Google* case has shown. Alongside deleting personal information, the user has an interest in not receiving intrusive advertisements. There are several browser extensions (e.g. Adblock plus) and products (e.g. eBlocker) for this purpose. However, one cannot access many websites once the extension is installed (unless one puts the site on a whitelist or subscribes to it). The reason is made clear, for instance, by the ToS of the online version of the magazine Forbes, under section 1.5, whereby "Free access to the content made available to you on the Website is possible due to the paid advertising that appears on the Website. Without this advertising, we would not be able to provide you with this content for free. In exchange for your free access to this content, you agree that *you will not, and will not permit any third party to, remove, obstruct, modify or otherwise interfere with the delivery or display of advertisements* on the Website".[151]

The importance of the issue has been (I suggest to delete given that the book will be published in 2018) confirmed by the battle between Facebook and Adblock Plus. On 9 August 2016, Facebook has released an ad block bypass, offering ad targeting opt-outs. In just two days, Adblock Plus has launched a workaround called FB-reblock. On the same day, the popular social network platform has reacted by rolling out the code update to disable Adblock Plus' workaround.[152] We are just at the beginning of a war and legislators and regulators intervene as usual too late to regulate the process.[153]

Google uses the DoubleClick cookie on publisher websites displaying AdSense[154] for content ads.[155] In theory, "DoubleClick cookies contain no personally identifiable information".[156] However, as said above, by recombining the information of the multiple devices of a user and the data relevant to the use of the services provided by Google and its partners, it is easy for the non-personal information to become personal and, hence, subject to data protection laws. The consent to these policies can hardly be considered meaningful, since the user is rarely aware of the data collection. Indeed, when the server delivers the ad content, it also sends a cookie.

[150] Caddy (2015).

[151] FORBES® Website Terms of Service, Revised and posted as of 5 November 2015, emphasis added, available at: http://www.forbes.com/terms.

[152] This is what a source close to Facebook told Constine (2016).

[153] This phenomenon can be called 'legal hysteresis' (Noto La Diega (2016b)).

[154] AdSense is an advertising placement service whereby website publishers earn money by displaying targeted Google ads on their websites. In turn, a business can advertise itself by using AdWords. The present analysis will focus on AdSense. However, one should be aware that Google also provides AdWords, Google Analytics and a range of DoubleClick-branded services.

[155] AdSense programme policies, last updated on 21 June 2016, available at: https://support.google.cm/adsense/answer/48182?utm_source=aso&utm_medium=link&utm_campaign=ww-ww-et-asfe_&hl=en-GB.

[156] DoubleClick cookies, available at: https://support.google.com/adsense/answer/2839090.

However, "a page doesn't have to show DoubleClick ads for this to happen; it just needs to include DoubleClick ad tags, which might load a click tracker or impression pixel instead".[157] One could object that all publishers must clearly display a privacy policy notifying visitors about the site's use of cookies. Nonetheless, it is common experience that it is customary the take it or leave it approach: either you accept the cookies policy by keep on surfing the site, or you can leave it. For instance, on 12 August 2016, this author first blocked all cookies and then tried to access the search setting preferences on Google Chrome, which sent him the following automatic message (Fig. 2 below).

Similar consequences occur for other Google services (e.g. Gmail),[158] but also on other websites, as seen above when discussing the review process of the ePrivacy Directive.

Furthermore, there is a risky obsession with consent in the public discourse on privacy. The truth is that there are several justifications for data controlling.[159] Consent is just one of them and requiring it for each and every kind of processing is cumbersome and hinders transparency and users' awareness. For instance, one of the several documents the user should be aware of is Google's EU user consent policy.[160] This requires the European user to express consent for each and every collection, sharing and use of data on every site or app. Provisions like this look more like privacy white-washing, rather than a serious commitment to privacy.

One should note, however, that Google requests that the publishers should not use AdSense "to facilitate the merging of personally identifiable information with information previously collected as non-personally identifiable information without robust notice of, and the user's prior affirmative (i.e. opt-in) consent to, that merger".[161] This invitation is commendable, but there is no evidence as to its implementation and, what is more important, the big data controlled by Google still

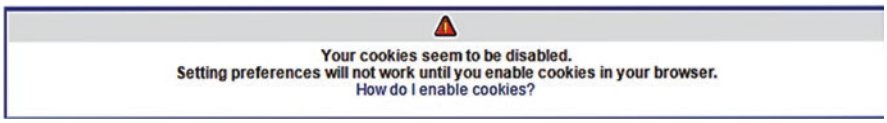


Fig. 2 Message shown by Google Chrome while accessing the search settings

[157] Ibid.

[158] On 12 August 2016, this author tried to access his Gmail account and was redirected to the page where cookies can be turned on (https://support.google.com/accounts/answer/61416?hl=en).

[159] As seen above, there are some actions for which informed consent is required (e.g. under Article 5(3) of the ePrivacy Directive).

[160] https://www.google.com/about/company/user-consent-policy.html.

[161] AdSense programme policies, which refer to a separate document named 'Best practices to avoid sending Personally Identifiable Information'. It is intended to provide guidance for complying with the Identifying Users Policy. See https://support.google.com/adsense/answer/6156630?ref_topic=6162392&rd=1.

enable the company to recombine personal and non-personal data to single out users. More generally, computer scientists and engineers have stressed that, even if many tools empower users to control whether and when they are tracked for targeted advertising,[162] "whether users can effectively control tracking and OBA using these tools is unclear".[163]

To add to the complexity, alongside the AdSense programme policies, there are additional policies for specific products, for instance AdMob, used for mobile applications. Its "Behavioural policies" deserve some attention. AdMob requires test ads in order to avoid invalid clicks and impressions. Accounts are disabled if Google finds such an invalid activity. The company analyses all clicks and impressions to determine whether they fit a pattern of use that might artificially drive up an advertiser's costs or a publisher's earnings. This approach is commendable; however, developments in artificial intelligence (e.g. machine learning) will render it more and more difficult to distinguish between machine/robot and human behaviour. Lastly, the policy states that "Google may use the advertising ID from the device on which the ad is being served to generate interests and demographics (for example, 'sports enthusiasts')". It further clarifies that "interests, demographics, and other data may be used to serve better targeted ads to the user". It is not clear which data these "other data" are. It probably refers to the targeting options, i.e. the parameters that make it possible to narrow down a mobile ad campaign to a specific audience. Unsurprisingly, AdMob is at the top of the list and it is the service with the highest number of targeting options, that is: country, region, carrier, connection type, mobile platform, OS version, device, audience (user profile data).

The AdSense programme policies and the product-specific policies, together with the Terms of Service (ToS),[164] form the agreement between the publisher and Google. As to privacy, the ToS refer to the general Google Privacy Policy,[165] which applies to all services provided by the company, unless otherwise stated.[166] The latter ensures that "[w]hen showing you tailored ads, we will not associate an identifier

[162] For a privacy-preserving tool see Pang et al. (2015), 1-8.

[163] Cranor (2012), 93.

[164] Google AdSense Online Terms of Service, available at: https://www.google.com/adsense/localized-terms?hl=en_GB. The contract between Google and the publishers is composed of (at least) three documents: the Google AdSense Online Terms of Service, the AdSense Programme Policies, and the Google Branding Guidelines. The AdSense programme policies are complemented by the EU consent policy, Deductions from Earnings FAQs, the Webmaster quality guidelines, the Ad implementation policies, the Content policies, the Product-specific policies and the Guidance for complying with the Identifying User Policy. Some of these policies are further fragmented. For instance, the Product-specific policies are divided into Behavioural policies, AdSense for video and games policies and AdSense for Search (AFS) policies. See also the Custom Search Engine Terms of Service.

[165] Privacy Policy, last updated on 26 June 2016, available at: https://www.google.it/intl/en-GB/policies/privacy/.

[166] There are specific privacy policies concerning Chrome and Chrome OS, Play Books, Payments, Fiber, Project Fi, and Google Apps Education Edition.

from cookies or similar technologies with sensitive categories, such as those based on race, religion, sexual orientation or health".[167] However, it is very easy to infer these data, for instance through an analysis of the searches on Google Search. For instance, if one searches for information about pills for a kidney disease, one will soon be shown relevant ads on one's social networking page.[168] Moreover, there is the issue of data recombination, as touched on above. Indeed, "your activity on other sites and apps may be associated with your personal information in order to improve Google's services and the ads delivered by Google".[169] Therefore, even if the ad is not supposed to collect personal information about the user, the personal information controlled by Google can be used for targeted advertising purposes. Google requires "opt-in consent for the sharing of any sensitive personal information",[170] in contrast with the Article 29 Working Party's opinion requiring opt-in mechanisms for all personal data (not only sensitive ones).

Furthermore, Google is not an island. It is part of a very intricate corporate structure and it partners with several companies. This can jeopardise privacy, as can be inferred by another passage of the privacy policy. Indeed, "Our Privacy Policy does not cover the information practices of other companies and organisations that advertise our services and that may use cookies, pixel tags and other technologies to serve and offer relevant ads."

Google is the strongest actor of the behavioural advertising world because it can monitor the users across several devices and services. The system feeds itself. In other words, if most of the advertisers, publishers, etc. use Google's services for advertising, at the same time they are providing Google with further data. Every time the user browses a website that does not belong to Google, but, for instance, uses AdSense, the +1 button of Google+, or Google Analytics, "your web browser automatically sends certain information to Google".[171] The same happens when using the apps that partner with Google.

On 13 September 2016, Google informed its users that there were some new features in their accounts. The declared purpose of the introduction was to give the user "more control over the data Google collects and how it's used, while allowing Google to show you more relevant ads".[172]

---

[167] Google privacy policy, last updated on 29 August 2016, available at: https://www.google.com/policies/privacy/.

[168] On 12 August 2016, this author googled 'kidney disease' and Adblock Plus blocked two relevant advertisements. Generally speaking, however, the protection afforded to sensitive personal data is high. See the experiment presented above in section 3.

[169] Google privacy policy.

[170] Ibid.

[171] How Google uses data when you use our partners' sites or apps, available at: https://www.google.it/intl/en-GB/policies/privacy/partners/.

[172] The notice is still available at: https://accounts.google.com/signin/newfeatures?cbstate=1&cbflow=promo-2-EN.

The first news is that more data will be available in the Google account. This includes all the data related to things the users search for, videos they watch on YouTube, and browsing data from Chrome,[173] as well as activity from sites and apps that partner with Google,[174] including those that show ads from Google. On the one hand, this is a lot of information, also because the new settings apply across all of the signed-in devices and across all Google services.[175] On the other hand, Google was already able to recombine the data produced by the use of all its different services. The news is that users now have a single place to review and control it. Moreover, Google is transparent as to the use they want to make of these data (and therefore, implicitly, of the *raison d'être* of the policy update): to serve more tailored advertisements.

Google also wants to increase its market power. Therefore, whereas now it can "only" use the data in "My Account" to tailor ads that appear in Google products, with the policy update the company will be allowed to leverage these big data also for targeted advertisements "on websites and apps that partner with Google".

Again, it is a huge amount of data. However, Google provides the users with the power to control and review its activity through "Web & App Activity" and "Ads Personalisation".

If the reader of the update wants to "Learn more", they will discover the real revolution behind the update: Google is sending cookies into retirement. Indeed, instead of serving ads based on a cookie ID for each device (which became quite useless in an Internet of Things era), "this change makes it possible to use a single identifier associated with your account that gets used in Google products and across the web".

Finally, it is commendable that there was no pre-ticked box (unlike the last WhatsApp policy update). One was able to choose between "I agree" and "Other options", which looked very straightforward (see Fig. 3 below).

[173] It is interesting that, with regard to the change concerning Chrome, Google points out that "[i]f you don't want to personalize your Google products, you can still use Google's cloud to store and sync your Chrome data without letting Google read any of your data. To add an additional layer of encryption, set up a sync passphrase" (https://support.google.com/chrome/answer/165139?p=personalization&visit_id=1-636098212979690973-579754209&rd=1#personalization).

[174] For instance, if a third-party app uses one of Google's services, say, Analytics, the app will send Google information about the user's behaviour, including "the name of the app and an identifier that helps us to determine which ads we've served to other apps on your device".

[175] Using "My Account" Google is actually overcoming the fragmentation of the Internet of Things by easily recombining data from multiple devices to identify a single user regardless of the point of access.

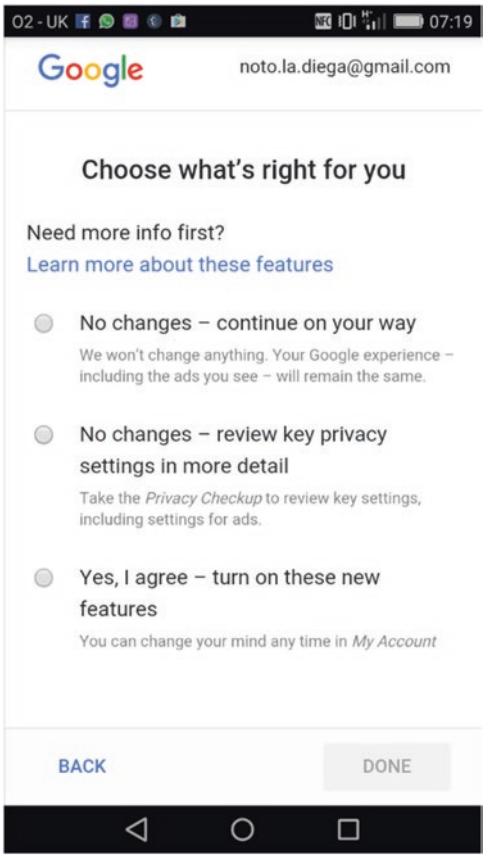


Fig. 3 Screen shown to Google users when accepting the changes in the privacy policy

6 The Use of Digital Assets to Hinder Competition. Facebook and WhatsApp: From the Concentration to the Transfer of the Latter's User Data to the Former's IP Portfolio

Companies (advertising networks, publishers, advertisers) can leverage the data in their IP portfolio to carry out unfair commercial practices and, more generally, to jeopardise competition.[176]

[176] The European regulation of competition in the field of advertising still defines targeted advertising as advertising targeted to a specific Member State, not the kind that singles out a user usually based on his or her behaviour. For instance, the ECJ stated that social, linguistic and cultural features specific to a given Member State, may cause consumers in that Member State to have a different interpretation of a product description used in commercial practice (ECJ, Case C-220/98, *Estée Lauder Cosmetics GmbH & Co. OHG v. Lancaster Group GmbH*, 13 January 2000, ECLI:EU:C:2000:8, para. 29). On 25 May 2016, the Commission adopted an updated version of

It is easily imaginable, for instance, that exploiting the users' data without their consent (or even awareness) or, more generally, using the users' data illegally does not merely damage consumers, but can also harm competitors. Also price discrimination and dynamic pricing based on profiling activities (e.g. offering a different price if one accesses a website from an old desktop than from an iPhone) might seem an unfair practice, but the Commission has clarified that under the Unfair Commercial Practices Directive[177] "traders are free to determine their prices if they duly inform consumers about the prices or how they are calculated".[178] However, some provisions of the said Directive do not really fit the reality of targeted advertising. For instance, under Art. 5(3), "[c]ommercial practices which are likely to materially distort the economic behaviour only of a clearly identifiable group of consumers who are particularly vulnerable to the practice or the underlying product […] in a way which the trader could reasonably be expected to foresee, shall be assessed from the perspective of the average member of that group". With current tracking and profiling techniques, it is unrealistic to allow for the possibility that a company might not be able to foresee the vulnerability of the target. Therefore, one should not look at the average member of the group, but at the single user. The definition itself of unfair commercial practices, with its reference to the average consumer, should be changed accordingly. One solution might be a presumption of vulnerability when it comes to targeted advertising, in consideration of the intrinsic characteristics of this kind of advertising.[179]

Another issue is the persistency of unwanted targeted advertisements. It is believed that this may be covered by Point No 26 of Annex I of the Unfair Commercial Practices Directive (on "Commercial practices which are in all circumstances considered unfair", which prohibits making persistent and unwanted commercial communications to consumers ('spam').[180] Lastly, it has been suggested that

---

the 2009 Guidance on the application of the Unfair Commercial Practices Directive. This seems to allow an extension to the new definition of targeted advertising, when the Commission observes that "[w]hen designing their commercial messages, traders may, at times and in light of the specific nature of the products at stake, need to take certain social, linguistic and cultural features into account which are typical of the average consumers to which the products are targeted" (European Commission (2016c), 45).

[177] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), OJ [2005] L 149. The Unfair Commercial Practices Directive is complemented, as regards business-to-business relations, by the Misleading and Comparative Advertising Directive.

[178] European Commission (2016c), 148.

[179] For a clear explanation of the functioning of the system with regard to the average consumer in the UK, see Department of Business Innovation & Skills (2014), para. 26 ff.

[180] The two main categories of unfair commercial practices are misleading practices and aggressive practices. Targeted advertising can be misleading inasmuch it is based on a deep knowledge of the consumers, hence allowing companies to exploit their weaknesses in order to mislead them. Targeted advertising may be aggressive as well. However, the wording of Art. 8 of the Unfair

"an undue increase in the use of personal data may very well be compared to excessive prices",[181] thus amounting, potentially, to a practice constituting abuse of dominant position.

As recently reaffirmed by the General Court in the first case of pay-for-delay in the pharmaceutical industry,[182] competition law can be used as a tool to prevent some of the IPRs holders' abuses. The below passages will assess if this could be the case in a recent event regarding the transfer of WhatsApp's users data to Facebook.

Harnessing the big data controlled by Facebook (directly and through its subsidiaries), the popular social networking platform can be considered one of the strongest actors in the targeted advertising world, especially considering its share of collected data across the web.[183] Indeed, in 2015, Facebook's advertising revenue was USD 17.08 billion.[184] Many approaches may be followed in choosing Facebook as a case study on targeted advertising. Here the focus will be on a mostly overlooked perspective, i.e. competition. There are many aspects of the Commission's decision[185] on the Facebook/WhatsApp concentration that offer a sample of the relevance of targeted advertising[186] from a competition law perspective. This decision, by the by, should be read again today in light of the use Facebook in August 2016 commenced making of WhatsApp users' data for targeted advertising purposes.[187]

Commercial Practices Directive is rather narrow, referring to "harassment, coercion, including the use of physical force, or undue influence [which] significantly impairs or is likely to significantly impair the average consumer's freedom of choice or conduct".

[181] Gebicka / Heinemann (2014), 165. However, as correctly pointed out by Surblytė (2015), 174, "although data could be considered the 'currency' of the Digital Economy in very general terms, it cannot precisely be equalled to the concept of a 'price".

[182] General Court, H. Lundbeck A/S and Lundbeck Ltd v. European Commission, T-472/13, ECLI:EU:T:2016:449. The Danish pharmaceutical company Lundbeck's basic patent for the blockbuster antidepressant medicine citalopram had expired. Some generic producers were, hence, preparing cheaper generic versions of citalopram. Therefore, in order to prevent competition, Lundbeck paid them not to enter into the market, thus harming patients and health care systems. This allowed Lundbeck to keep the price of its blockbuster drug citalopram artificially high. Consequently, upholding the Commission's decision, the General Court found that the agreements eliminated the competitive pressure from the generic companies and were "a restriction of competition by object". The examples of use of competition law to limit IPRs are myriad, but the classic example is exhaustion.

[183] As noted by Surblytė (2015), 174, the quantity of data can become quality insofar as "the volume of data counts when it comes to the quality of search results, which may improve based on the economies of scale".

[184] See the summary of the relevant statistics at: http://www.statista.com/statistics/234056/facebooks-average-advertising-revenue-per-user/.

[185] European Commission, Case M.7217 – Facebook/ WhatsApp, 3 October 2014.

[186] The decision refers mainly to 'online advertising' in general, but given that the company involved carries out mainly targeted advertising, the author believes that the Commission's 2014 decision constitute a good prism through which to observe the competition implications of targeted advertising.

[187] https://www.whatsapp.com/legal/#key-updates.

To briefly recap the facts, in the summer of 2014, the European Commission received notification of a proposed concentration pursuant to Article 4 of the Merger Regulation, and following a referral pursuant to Article 4(5) of the Merger Regulation, by which Facebook, Inc. acquired within the meaning of Article 3(1)(b) of the Merger Regulation control of the whole of WhatsApp Inc. by way of purchase of shares (the "Transaction"), for a price of USD 19 billion.

One of the main differences between Facebook and WhatsApp is that the former provides online advertising services, the latter does not. One could have been surprised by the news of the transaction, given that Facebook already had its own instant messaging app, Messenger. In assessing the closeness to competition, however, the Commission explains that Messenger is a stand-alone app that was developed from functionalities originally offered by the Facebook social network. From the above, some differences follow. According to the Commission, one of them is that, contrary to WhatsApp, "Messenger enables Facebook to collect data regarding its users that it uses for the purposes of its advertising activities".[188] This is no longer the case after the update to the "legals" of WhatsApp occurred on 25 August 2015.[189] The main news is that Facebook will use the WhatsApp account information for targeted advertising purposes. What is worse is that: 1. The chosen mechanism is an opt-out one (see Fig. 4 below[190]). 2. The opt-out procedure is not straightforward.[191] 3. The users have only 30 days after the update to opt out. 4. New users have no right to opt out. Especially the last bit seems hardly enforceable.

Finally, it is not clear which information Facebook will be able to use. Indeed, even though in the "key updates" recap, WhatsApp refers only to the account information, the new ToS state:

> Facebook and the other companies in the Facebook family also may use information from us to improve your experiences within their services such as making product suggestions (for example, of friends or connections, or of interesting content) and showing relevant offers and ads. However, your WhatsApp messages will not be shared onto Facebook for others to see. In fact, Facebook will not use your WhatsApp messages for any purpose other than to assist us in operating and providing our Services.

[188] European Commission, Case M.7217 – Facebook/ WhatsApp, 3 October 2014, para. 102.

[189] https://www.whatsapp.com/legal/#terms-of-service and https://www.whatsapp.com/legal/#privacy-policy. For the previous versions, see https://www.whatsapp.com/legal/?doc=terms-of-service&version=20120707 and https://www.whatsapp.com/legal/?doc=privacy-policy&version=20120707. In the former version of the terms, no reference was made to advertising (be it that of Facebook or of WhatsApp). In the previous privacy notice, in turn, it was stated: "[w]e are (not fans of advertising). WhatsApp is currently ad-free and we hope to keep it that way forever. We have no intention to introduce advertisements into the product, but if we ever do, we will update this section".

[190] This pre-ticked box appeared on the screen of this author's phone on 26 August 2016 at 8:51 GMT.

[191] Cf. Lomas (2016).

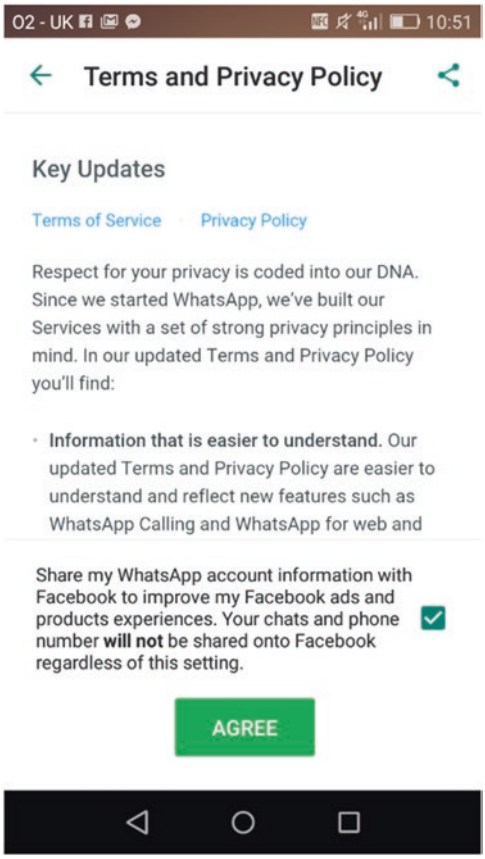


Fig. 4 Screen shown by WhatsApp when communicating the change in privacy policy consisting in the sharing of data with Facebook

The wording suggests that WhatsApp messages are not shared, but all the rest of information can be used (and shared). This includes, for instance, phone number, profile name, and photo.

With regard to the assessment of whether Facebook and WhatsApp were direct competitors, the Commission found that they were not and therefore authorised the concentration. It can be argued that, if the Commission was notified today of the said transaction, the conclusion would be different. Indeed, at that time the Commission considered Facebook as in direct competition with Twitter or Google Hangouts, but not with WhatsApp, which was in turn closer to Viber.[192] However, if one of the main differences between Facebook Messenger and WhatsApp was that the latter's data were not used for the advertisements served by the former, which is no longer the case, it is clear that the forecast capabilities of the Commission failed.

[192] European Commission, Case M.7217 – Facebook/ WhatsApp, 3 October 2014, paras 106-107.

Whereas other "free" consumer communications apps monetise by using advertising, in-app purchases, and stickers, "Messenger is not currently monetised: it is funded by the monetisation of Facebook's networking platform through advertising".[193] Therefore, it is to be believed that the use of the data created through the use of Messenger is the main reason for the existence itself of this app. This could be criticised, since users are hardly aware of their private conversations being exploited for targeted advertising purposes. It is not by chance that, as seen above, this has been the subject of a written question to the Commission.[194]

In the concentration, there are three relevant markets: consumer communications services, social network platforms, and online advertising. The latter is of main interest here.

Facebook's activities in the advertising sector consist in the provision of online (non-search) advertising services on Facebook's core social networking platform and on Instagram[195] (which is its subsidiary as well), both on computers and on mobile devices. As noted above in the case of Facebook and Mrb&b, Facebook collects its users' data (also through its subsidiaries[196]) and analyses them in order to serve targeted advertisements on behalf of advertisers.

The Commission has investigated the market definition as regards advertising. The product market definition is quite straightforward. Following its precedent assessments,[197] the Commission distinguishes between the provision of online and offline advertising space. The market investigation carried out in the Facebook / WhatsApp case supported the existence of a further sub-segmentation of the online advertising market between search and non-search advertising. Indeed, most advertisers see search and non-search ads as non-substitutable, since they serve different purposes (search advertisements mainly generate direct user traffic to the merchant's website, while non-search advertisements mainly build brand awareness).[198]

---

[193] Ibid., fn 42.

[194] Tarabella (2013).

[195] See the section on "Rights", § 2 of Instagram Terms of Use, effective as of 19 January 2013, available at: https://help.instagram.com/478745558852511: "Some of the Service is supported by advertising revenue and may display advertisements and promotions, and you hereby agree that Instagram may place such advertising and promotions on the Service or on, about, or in conjunction with your Content. The manner, mode and extent of such advertising and promotions are subject to change without specific notice to you".

[196] Facebooks owns Instagram, WhatsApp, PrivateCore, and Oculus VR.

[197] European Commission, Case M.5727 – Microsoft / Yahoo! Search Business, 18 February 2010, para. 61; European Commission, Case M. 4731 – Google / DoubleClick, 11 March 2008, paras 45-46; 56.

[198] European Commission, Case M.7217 – Facebook/ WhatsApp, 3 October 2014, para. 76.

From our perspective, what is more relevant is the assessment with regard to a further sub-sub-segmentation. Indeed, the Commission examined whether a separate product market should be defined for the provision of online non-search advertising services on social networking websites. A number of respondents considered that other forms of non-search advertising are not as effective as advertising on social networking websites and "notably on Facebook, due to Facebook's large and highly engaged audience and its ad targeting opportunities".[199] Nonetheless, the Commission decides to leave to question open "because the Transaction would not give rise to serious doubts as to its compatibility with the internal market under any[200] such narrower product market definition".[201]

Therefore, from a product perspective, the relevant market is online advertising. As to the geographic market, most respondents to the Commission's market investigation stated that advertisers typically purchase online advertising space and conduct advertising campaigns on a national (or linguistic) basis.[202] Therefore, In line with the *Google / DoubleClick* and *Microsoft / Yahoo! Search Business* decisions, the Commission concluded that the online advertising market and its possible subsegments should be defined as national in scope or alongside linguistic borders within the EEA.[203]

The Commission exposed itself to criticism by taking a rather formalistic approach,[204] rigidly distinguishing between a competition law approach and a privacy law approach, whereas a holistic one would have been appropriate. The Commission seems to imply that there may be privacy concerns emerging from the merger, but this is not a matter for competition law, which deals merely with the likeliness that the data concentration strengthens Facebook's position in the online advertising market. If it is true that, generally speaking, not every privacy-threatening merger is anti-competitive, given the growing importance of data as commodities, such a formalistic approach should not be taken. On the contrary, the Commission should assess on a case-by-case basis whether there is an overlap. This seemed to be the case in 2014 and is all the more true now, after the terms update of 25 August 2016. It has, indeed, become clear that one of the main ways Facebook is profiting from the authorised merger is in its access to the gigantic amount of data once controlled by WhatsApp. At any rate, even if the Commission continued to adopt the

[199] Ibid., para. 77.

[200] Another question which has been left open regards a possible distinction between online advertising on different platforms (essentially on computers or on mobile devices).

[201] European Commission, Case M.7217 – Facebook/ WhatsApp,3 October 2014, para. 79.

[202] However, a number of respondents also pointed out that, depending on the type of campaign, global companies may also procure advertising space on a broader (sometimes global) geographic scale.

[203] European Commission, Case M.7217 – Facebook/ WhatsApp, 3 October 2014, para. 83.

[204] "Any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules" (European Commission, Case M.7217 – Facebook/ WhatsApp, 3 October 2014, para. 164).

said formalistic approach, if the Commission had to decide on this case today, one could expect that the merger would not be authorised. Indeed, it is no longer true that the "transaction does not increase the amount of data potentially available to Facebook for advertising purposes".[205]

However, the Commission also assessed the possibility that, in the future, Facebook would start using WhatsApp users' data for targeted advertisements served on the social network platform. The Commission ended up espousing Facebook's allegations whereby: 1. "the data that WhatsApp has access to is at best of marginal utility for Facebook's advertising purposes and would not enhance Facebook's ability to target advertisements on its services"[206]; 2. "Facebook has publicly made it clear that it has no current plans to modify WhatsApp's collection and use of user data"[207]; 3. The CEO of WhatsApp commented by saying that privacy was in its company's DNA and that "if partnering with Facebook meant that we had to change our values, we wouldn't have done it"[208]; 4. Facebook pointed out, debatably, that it was technically nearly impossible "to match each user's WhatsApp profile with her/his Facebook profile"[209]; 5. There was no incentive to use the WhatsApp users' data, because this would lead them to abandon the famous app in favour of more privacy-friendly competitors such as Telegram. It can be said that some or all of these assertions were wrong. For instance, the last statement ignores some basic concepts such as lock-in and network effect. However, what is decisive is that, given the leading position of Google (also) in the online advertising market, the only merger that would probably not be authorised is the Google/Facebook one.

As a brief note on the aftermath: in September 2016 the European Commissioner for Competition Margrethe Vestager declared that she has asked some follow-up questions to Facebook, in relation to the change of WhatsApp's privacy policy. The Commissioner declared: "[t]hat they didn't merge data wasn't the decisive factor when the merger was approved, but it was still a part of the decision".[210] We do not know yet how the story will end, nor does the Commissioner, who leaves the social network and us in the dark by saying that "[w]hat we're going to do with the answers we get is still an open question".[211]

---

[205] Ibid., para. 166.

[206] Ibid., para. 181.

[207] Ibid., para. 182.

[208] http://blog.whatsapp.com/529/Setting-the-record-straight.

[209] European Commission, Case M.7217 – Facebook/ WhatsApp, 3 October 2014, para. 185.

[210] White / Levring (2016).

[211] Ibid.

7 Conclusions. A More Balanced Approach to Data as Digital Assets and the "Cooperative Charter on Online Behavioural Advertising"

Targeted advertising can be a positive phenomenon, inasmuch as it helps the user experience to be less disrupted by irrelevant advertisements. On the other hand, there can be several problems for the consumer, for instance in terms of price discrimination, influence on voting preferences, distress at having the (well-grounded) feeling that one cannot really escape the advertising net. The principles at stake are of the highest importance; they include autonomy[212] and self-determination.[213] The best consumers are the most predictable ones, and it is understandable why companies are doing their best to influence our present and future behaviour in subtler and subtler ways, especially through subliminal messages[214] and machine learning algorithms to which users do not have access. At the same time, however, it is not possible to ban targeted advertising by saying that it conflicts with data protection, privacy, and consumer protection. As mentioned above, if the targeted advertising is effective, data protection laws will apply, because the clear purpose of the former is to single out a consumer. Banning targeted advertising altogether would be contrary to the principles of competition and freedom of enterprise and it would jeopardise one of the biggest assets in the IP portfolio of a great many companies.

The approach being taken to data in Europe is far from holistic. Leaving aside the rhetoric of fundamental and human rights, it is apparent that most regulators take account of data only from a perspective of privacy and data protection, thus showing their failure to understand the role of data as digital assets.[215] Probably, if citizens were aware of the economic value of their data, and if data were treated as their intellectual property,[216] then they would care more about the information they

[212] Especially when we try to ignore the ads, the effects of so-called affective conditioning increase. We do not freely choose a product because it is the best one, but because the advertising has paired it with positive items, thus creating a false desire for a product, regardless of its intrinsic characteristics. According to Dempsey / Mitchell (2010), 622, this "can occur even when consumers have both the motivation and the opportunity to retrieve product attribute information from memory".

[213] The problem is not limited to targeted advertising, but applies to the more general online aspect of our everyday life, especially with regard to the Internet of Things. To put it in the alarming words of Michael (2016), 20, "We are losing our ability to make decisions for ourselves, to make a choice based on our preferences, not imposed by computer systems.".

[214] Cf. Merikle (2000), 497.

[215] With regard to other topics, a similar conclusion is proposed by Mik (2016).

[216] One may object to this proposal because data do not fall easily under the traditional IP categories (copyright, designs, patents, trademarks). However, many developments show how the IP paradigm is evolving, becoming simpler and more comprehensive. For instance, in the UK, trade secrets are protected through the breach-of-confidence rule, usually in combination with contract law. The *Vidal-Hall v Google* case is a reminder of how hard it is to draw a clear line between data

share.[217] The legal tools introduced over the years by lawmakers and regulators under the data protection umbrella have proven to be quite easily circumventable by online intermediaries, public bodies, and hackers. The developments concerning targeted advertising confirm this insight. Therefore, to empower the citizens in their online dimension, as well as in the offline one, this chapter calls on lawmakers, regulators, judges, and academics to embrace a shift of paradigm. Too many times compliance with the data protection rules has proven to be impossible or fictitious (the ePrivacy Directive with its mechanism on cookies provides robust evidence of this). Data protection laws should be simplified and informed by a holistic interplay of data protection, intellectual property, consumer protection, and competition. There are at least two reasons to do this. Firstly, in a world where the economy is global and space is virtual, it is not possible for all the national systems to demand compliance with their own (sometimes radically different) rules.[218] Secondly, like it or not, data have become the crucial commodity for countless markets and companies.

Opt-in mechanisms would provide a stronger protection for users, but the international and European self-regulatory frameworks have made clear that there is no chance that companies will voluntarily adopt the opt-in mechanism. At the same time, the ePrivacy Directive shows how useless certain legal burdens based on pure consent can be. Hence, one may take a pragmatic approach and try to make the former method work.

Therefore, it is proposed the following "Cooperative Charter on Online Behavioural Advertising"

protection, breach of confidence, and misuse of private information (the first and the last are torts, while with the second it is not entirely clear whether it has its roots in contract, property, tort, or equity, or is a *sui generis* action). Moreover, the Intellectual Property Office (2016) 18 has shown that the most popular means to protect immaterial assets in the UK is the confidentiality agreement, which does not really fit in any traditional IP category.

[217] Nonetheless, see the concerns expressed by Drexl et al. (2016) as to creation of new exclusive rights in data "which could even hamper the functioning of the data-driven economy". The authors' concerns, however, are mainly due to the fact that intellectual property of data is seen only from the perspective of those who commercially exploit the users' data. This chapter's stance takes the viewpoint of users and it would like to entrust them with the ownership of data. It is believed that data are already de facto treated as digital assets: the main aim of the proposal is to broaden the audience of data owners to include their subjects.

[218] Cf. Reed (2016) and his proposal of a new concept of legitimacy.

Article 1
Users have the right to opt out from online[219] advertising altogether, as well as from its single types.[220] Circumvention of these measures is in breach of the ePrivacy Directive, of the Unfair Commercial Practices Directive, as well as general tort laws. If the circumvention is grounded on a contract, the Directive on unfair terms in consumer contracts shall apply, in case of business-to-consumer transactions.

Article 2
Users have the right to know which companies are tracking, profiling, and serving advertisements to them. They have the right to know the basis whereupon the advertisements are served,[221] as well as the purpose for which data are used, the retention time, and the measures put in place to comply with applicable laws. All information is provided in a brief, clear, and gamified[222] way.

Article 3
Companies are held accountable for the algorithmic decision-making occurring with regards to the services provided. Accountability includes transparency on the reasoning of the artificial agents.

Article 4
Personal data are digital assets in the data subjects' intellectual property portfolios. Users can issue data licenses, which can be terminated at any time. Personal data cannot be assigned and the relevant remedies cannot be excluded by means of a contract.

[219] The characteristics of online advertising make the "change the channel" remedy often unviable.

[220] Users should be made aware, for instance, that the opt out from interest-based advertising might still allow some form of OBA.

[221] Including, for instance, when and where they have consented, which data were used to serve it, etc.

[222] Gamifying privacy seems pivotal to making users take privacy seriously. Indeed, given the tendency not to read the privacy policies, gamification can lead to increased interactivity and thus alertness. See, for instance, Centre for Democracy and Technology 'The Gamification of Privacy' (2011), https://cdt.org/blog/the-gamification-of-privacy/. Some authors distinguish between serious games and gamified interactions (Rottondi and Verticale (2017), 14221). The former refers to games designed for purposes others than entertainment, the latter to "the use of game design elements in non-game contexts". In this paper, it is believed that using game design elements in the drafting and presentation of privacy policies can be a good way to increase the users' awareness thus making it more likely that they will have privacy-preserving behaviours. Unlike Rottondi and Verticale (2017), 14221, this chapter is more concerned with the use of games to protect privacy, rather than with the privacy risks of online gaming.

Article 5
Companies responsible for online behavioural advertising (primarily, advertising networks, publishers, advertisers) act in good faith.[223] Good faith and transparency pose inter alia an obligation to provide information in a brief, clear, and interactive gamified way also beyond the scope of Article 2 of this Charter.

Article 6
If feasible with regards to the development of the technologies involved, companies use the data collected in connection to online behavioural advertising in order to put in place forms of bespoke legal compliance. Online behavioural advertising carried out without the users' awareness is unlawful. These technologies are developed also with the purpose of increasing said awareness.[224]

Article 7
Companies make available optional[225] online dispute resolutions, and refrain from mandatory binding arbitration.

One can (and has to) require transparency, accountability, and good faith in the handling of the private information, but closing all the valves will only make the dam burst.

There are some technical as well as legal tools that can enhance privacy in an environment of ubiquitous surveillance, like the one necessary for targeted advertising to thrive. Some of these means can be easily circumvented (see the AdBlock Plus v Facebook war) or are more apparent than real (see the experiment on the consequences of blocking all cookies).[226] Tracking and profiling, however, are not all bad. For some time, this author used DuckDuckGo, the search engine famous for not tracking users. The problem was that the results of the searches were utterly useless. To receive suggestions of music we can enjoy on YouTube, to be shown news we are interested in or search results that answer our questions precisely, badly formulated though they can sometimes be: these are some of the reasons why

[223] This means, in the first place, to ensure the right to dissent by, for example, not circumventing ad-blockers and browser settings which block OBA. See the recently amended Article L. 111-7(II) of the *Code de la consommation*, which provides that "Tout opérateur de plateforme en ligne est tenu de délivrer au consommateur une information loyale, claire et transparente,".

[224] For instance, instead of pre-ticking the "I have read/I have understood" boxes, providers should pre-tick an "I have not read/I have not understood" box. The concept of "awareness by design" was introduced in Noto La Diega (2016a), 24, where it is defined broadly as "the use of technologies (especially design) to empower the user and make them aware of risks, rights, and obligations".

[225] One of the main problems in Internet-related disputes is the attempt of online platforms and other strong intermediaries to prevent the access to public justice by means of compulsory alternative dispute resolution. It is a problem that goes beyond OBA, but this could be the opportunity to address the issue.

[226] More generally, as observed by Hoofnagle et al. (2012), 273, "the combination of disguised tracking technologies, choice-invalidating techniques, and models to trick the consumers into revealing data suggests that advertisers do not see individuals as autonomous beings".

machine learning-enabled and predictive, analytics-based algorithmic decision-making can improve the quality of our lives.[227] Even targeted advertising, if freely and actively chosen, with the possibility to withdraw one's consent any time, can reduce our search costs, thus making our life easier. Letting users understand that their data are a critical digital asset of their IP portfolio is a good way to raise awareness and increase the quality of data flows and the overall satisfaction of all the actors of the market. The awareness of the pros and cons of this practice should be kept in mind by courts and regulators that are called upon to protect users' privacy, but also to strike a balance between that privacy and intellectual property, free competition, and consumer protection.

> The GDPR constitutes a step forward as compared with the Data Protection Directive, but much will depend on the revision of the ePrivacy Directive and on the adoption of the Cooperative Charter on Online Behavioural Advertising. Hopefully, algorithmic accountability and transparency, the right to dissent, gamified interactions and the right to disconnect will be the North Star that the online sailors follow.[228]

8 Afterword. Of Chocolate Chips and Lavender Buds

I recently came across a story that deserves to be shared, because it reminds us to avoid any kind of simplism and invites us to adopt more nuanced approaches when it comes to our online lives.

Amy and her husband had long tried to conceive, unfortunately without success. Therefore, when the magenta plus sign materialised on the stick, they were overwhelmingly happy. On the day of the positive pregnancy test, Amy logged into her period tracker to share the good news. The tracker suggested a pregnancy app that Amy downloaded. It was very entertaining and sweet, it showed the evolutions of the baby, who initially was the size of a lavender bud. Alas, when the baby had reached the stage of the chocolate chip, Amy miscarried. Once home from the clinic, Amy terminated her virtual pregnancy with the touch of a button. The app responded with a soothing email and cleared her data. Harsh times followed, understandably,

[227] There is a number of cons. One of them is social network homophily, that is, the fact that we listen and speak only to the like-minded while online, with the risks of "excessive confidence, extremism, contempt for others, and sometimes even violence" (Sunstein (2007), 10). Along the same lines, it has been said that algorithms used to rank search results and social media posts create "filter bubbles," in which only ideologically appealing content appears (Pariser (2011)). Bakshy et al. (2015), 1-4, have presented evidence that people are exposed to a substantial amount of content from friends with opposing viewpoints.

[228] This solution empowers the user, whereas most solutions focus on the role of the public institutions and on regulation. Along those lines, for instance, see Klein (2016), 19, according to whom, given that corporations have no real incentive to protect privacy, "it is time to think about independent, international, publicly funded, and democratically legitimized institutions to either run and provide, or at least oversee and finance the lower level digital infrastructures, the social networks, and the messaging apps, etc., that we rely on as well". The premise is acceptable, less so the top-down solution.

when one day a parcel arrived. Seven months after the miscarriage, Amy received a box of baby formula bearing the note: "We may all do it differently, but the joy of parenthood is something we all share." A product she had never intended to use from people she had never told she was pregnant at a company she had never heard of. The period tracker had shared, that is to say sold, her data to providers of products for mothers. One's instinct, in reading this story, could be to react with a sense of repulsion and by condemning tracking, profiling, and direct marketing altogether. However, if tracking, profiling, and direct marketing had worked properly, this unfortunate event would not have happened. If the reader is wondering how the story ends, it is with a bitter laugh. When Amy received the box, she laughed. Indeed, on the one hand, she "liked the idea that a data-hungry entity like the internet, which is so intimately involved in every trivial aspect of our lives, had completely missed the most important news of all".[229] On the other hand and more importantly, she realised that her "little chocolate chip, long since deleted, is indeed out there somewhere, drifting around in cyberspace, endlessly trolling the internet".[230]

References

Article 29 Working Party (2011), Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising, adopted on 8 December 2011, 02005/11/EN WP 188, European Commission

Article 29 Working Party (2010), Opinion 2/2010 on online behavioural advertising, adopted on 22 June 2010, 00909/10/EN WP 171, European Commission

Article 29 Working Party and Working Party on Police and Justice (2009), The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, adopted on 1 December 2009, 02356/09/EN WP 168, European Commission

Ask Your Target Market (2011), Targeted Advertising Survey: Many Worried About Privacy Violations, Aytm.com of 20 December 2011, available at: https://aytm.com/blog/daily-survey-results/targeted-advertising-survey/#sthash.3rEVQvsg.dpbs

Ayenson, Mika, Dietrich Wambach, Ashkan Soltani, Nathan Good, and Chris Hoofnagle. "Flash cookies and privacy II: Now with HTML5 and ETag respawning." (2011)

Bakshy, E. / Messing, S. / Adamic, L. (2015), Exposure to ideologically diverse news and opinion on Facebook, in: SciencExpress of 7 May 2015, available at: http://cn.cnstudiodev.com/uploads/document_attachment/attachment/681/science_facebook_filter_bubble_may2015.pdf

Bauer, C. / Eickmeier, F. (2016), GDPR: What's Relevant for the Use of Cookies & Identifiers in Online Marketing, ExchangeWire of 24 May 2016, available at: https://www.exchangewire.com/blog/2016/05/24/gdpr-whats-relevant-for-the-use-of-cookies-identifiers-in-online-marketing/

Bauer, C. / Breuer, M. / Diebold, D. / Eickmeier, F. / Klekamp, J. / Maucher, S.-A. / Neuber, N. / Rackwitz, G. / Wegmann, T. (2015), Browsercookies und alternative Tracking-Technologien: technische und datenschutzrechtliche Aspekte, BVDW Whitepaper of September 2015, available at: http://www.bvdw.org/medien/browsercookies-und-alternative-tracking-technologien-technischeund-datenschutzrechtliche-aspekte?media=7007

[229] Pittman (2016).

[230] Ibid.

Bernal, P. (2012), Phorm – A chapter closes?, Blog post of 28 January 2012, available at: https://paulbernal.wordpress.com/2012/01/28/phorm-a-chapter-closes/

Bray, O. / Griffiths, S. (2008), Information Commissioner's Office opinion on Phorm's targeted advertising technology, World Data Protection Report 2008, 8(6), 24-26

Caddy, B. (2015), Google tracks everything you do: here's how to delete it, Wired of 15 October 2015, available at: http://www.wired.co.uk/article/google-history-search-tracking-data-how-to-delete

Calabrese, C. / McInnis, K.L. / Hans, G.S. / Norcie, G. (2015), Comments for November 2015 Workshop on Cross-Device Tracking, Letter of the Center for Democracy & Technology to the Federal Trade Commission of 16 October 2015, available at: https://cdt.org/files/2015/10/10.16.15-CDT-Cross-Device-Comments.pdf

Chamberlain, P. (2015), Misuse of private information: Google Inc v Vidall-Hall & Ors [2015] EWCA Civ 311, 20(3) Communications Law 93

Commission of the European Communities (1995), Report on application of Directive 89/552/EEC and Proposal for a European Parliament and Council Directive 89/552/EEC on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities, COM(95)86 final 95/0074 (COD)

Constine, J. (2016), Facebook rolls out code to nullify Adblock Plus' workaround, TechCrunch of 12 August 2016, available at: https://techcrunch.com/2016/08/11/friendblock/

Coutts, S. (2016), Anti-Choice Groups Use Smartphone Surveillance to Target 'Abortion-Minded Women' During Clinic Visits, Rewire of 25 May 2016, available at: https://rewire.news/article/2016/05/25/anti-choice-groups-deploy-smartphone-surveillance-target-abortion-minded-women-clinic-visits/

Cranor, L.F. (2012), Can Users Control Online Behavioral Advertising Effectively?, 2 IEEE Security & Privacy, 2012, 93

Cufoglu, A. (2014), User Profiling - A Short Review, International Journal of Computer Application 2014, 3, 1-9, Foundation of Computer Science

De Hert, P. / Papakonstantinou, V. (2016), The new General Data Protection Regulation: Still a sound system for the protection of individuals?, 32(2) Computer Law & Security Review 179.

Dempsey, M.A. / Mitchell, A.A. (2010), The Influence of Implicit Attitudes on Choice When Consumers Are Confronted with Conflicting Attribute Information, Journal of Consumer Research 2010, 37, 4, 614-625

Department of Business Innovation & Skills (2014), Misleading and Aggressive Commercial Practices – New Private Rights for Consumers. Guidance on the Consumer Protection (Amendment) Regulations 2014, August 2014, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409334/bis-14-1030-misleading-and-aggressive-selling-rights-consumer-protection-amendment-regulations-2014-guidance.pdf

Díaz-Morales, R. (2015), Cross-Device Tracking: Matching Devices and Cookies, 2015 IEEE International Conference on Data Mining Workshop (ICDMW), 2015, 1699-1704

Drexl, J. / Hilty, R. / Desaunettes, L. / Greiner, F. / Kim, D. / Richter, H. / Surblytė, G. / Wiedemann, K. (2016), Data Ownership and Access to Data - Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate. Max Planck Institute for Innovation & Competition Research Paper No. 16-10, available at: https://ssrn.com/abstract=2833165

Eggers, W. / Hamill, R. / Ali, A. (2013), Data as the new currency: Government's role in facilitating the exchange, Deloitte Review 2013, 13, 19-29

European Advertising Standards Alliance (2015a), Cross-Border Complaints Quarterly Report no. 68 April – June, available at: http://www.easa-alliance.org/sites/default/files/2015%20EASA%20Cross-Border%20Complaints%20Report%20No.%2068.pdf

European Advertising Standards Alliance (2015b), Cross-Border Complaints Quarterly Report no. 67 January – March, available at: http://www.easa-alliance.org/sites/default/files/2015%20EASA%20Cross-Border%20Complaints%20Report%20No.%2067.pdf

European Advertising Standards Alliance (2014), Cross Border Complaints Report, available at: http://www.easa-alliance.org/sites/default/files/2014%20EASA%20Annual%20Cross-Border%20Complaints%20Report.pdf

European Advertising Standards Alliance (2011), Best Practice Recommendation on Online Behavioural Advertising, 13 April 2011, available at: http://www.edaa.eu/wp-content/uploads/2012/10/EASA_BPR_OBA_12_APRIL_2011_CLEAN.pdf

European Interactive Digital Advertising Alliance and TRUSTe (2015), European Advertising Consumer Research Report 2015. Consumer Awareness & Impact of European Self-Regulatory Programme for OBA, available at: https://www.dropbox.com/s/2wueligxquyn5mm/EDAA-TRUSTe_2015%20Consumer%20Research%20Report.pdf?dl=0

European Commission (2016a), Summary report on the public consultation on the Evaluation and Review of the ePrivacy Directive, 4 August 2016, available at: https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-evaluation-and-review-eprivacy-directive

European Commission (2016b), Commission Staff Working Document on Online Platforms, Accompanying the document Communication on Online Platforms and the Digital Single Market {COM(2016) 288 final}, SWD(2016) 172 final

European Commission (2016c), Commission Staff Working Document "Guidance on the implementation/application of Directive 2005/29/EC on unfair commercial practices". Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "A comprehensive approach to stimulating cross-border e-Commerce for Europe's citizens and businesses {COM(2016) 320}", SWD(2016) 163 final

European Commission (2016d), Commission Staff Working Document "Impact Assessment on the modernisation of EU copyright rules". Accompanying the document "Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market" and "Proposal for a Regulation of the European Parliament and of the Council laying down rules on the exercise of copyright and related rights applicable to certain online transmissions of broadcasting organisations and retransmissions of television and radio programmes" {COM(2016) 593} {COM(2016) 594} {SWD(2016) 301}, SWD(2016) 302 final

European Data Protection Supervisor (2011a), EDPS calls on the European Commission to ensure that safeguards for online behavioural advertising are respected, Press release of 11 July 2011, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/PressNews/Press/2011/EDPS-2011-08_Behavioural%20advertising_EN.pdf

European Data Protection Supervisor (2011b), Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions — 'A comprehensive approach on personal data protection in the European Union', 2011/C 181/01, Official Journal of the European Union of 22 June 2011 C 181/1

European Data Protection Supervisor (2010), Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, 2010/C 280/01, Official Journal of the European Union of 16 October 2010 C 280/1

Evans, K. (2015), Vidal-Hall and Risk Management for Privacy Breaches, 13(5) IEEE Security & Privacy 80

Fan, Y.C. / Chen, Y.C. / Tung, K.C. / Wu, K.C. / Chen, A.L.P. (2016), A Framework for Enabling User Preference Profiling through Wi-Fi Logs, IEEE Transactions on Knowledge and Data Engineering, 3, 592-603, IEEE

Federal Trade Commission (2009), Self-Regulatory Principles for Online Behavioral Advertising, FTC Staff Report of February 2009, available at: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf

Flint, D. (2016), Computers and Internet: what is the value of personal data? 37(1) Business Law Review (UK) 38

Gebicka, A. / Heinemann, A. (2014), Social Media & Competition Law, 37(2) World Competition 149

Gibbs, S. (2016), Facebook will delete your backed-up photos if you don't install Moments app, The Guardian of 13 June 2016, available at: https://www.theguardian.com/technology/2016/jun/13/facebook-delete-photos-moments-app

Graham, N. / Anderson, H. (2008), Phorm: the legality of targeted advertising, 10(4) E-Commerce Law & Policy 1

Groom, S. (2014), Spam judgment against John Lewis highlights limits of soft opt-in and ICO Guidance, but questions remain, Osborne Clarke Marketing Law of 18 June 2014, available at: http://marketinglaw.osborneclarke.com/data-and-privacy/spam-judgment-against-john-lewis-highlights-limits-of-soft-opt-in-and-ico-guidance-but-questions-remain/

Hoofnagle, C.J. / Soltani, A. / Good, N. / Wambach, D.J. / Ayenson, M.D. (2012), Behavioral Advertising: The Offer You Cannot Refuse, 6 Harvard Law & Policy Review 273

Hustinx, P. (2011), Do not track or right on track? – The privacy implications of online behavioural advertising, Speech of 7 July 2011, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2011/11-07-07_Speech_Edinburgh_EN.pdf

Information Commissioner's Office (2016), Overview of the General Data Protection Regulation (GDPR), 7 July 2016

Information Commissioner's Office (2011), Personal Information Online Code of Conduct, v.2.0

Intellectual Property Office (2016), Intellectual Property Awareness Survey 2015, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/500211/IP_awareness_survey_2015.pdf

Interactive Advertising Bureau (2011), Europe EU Framework for Online Behavioural Advertising, April 2011, available at: http://www.edaa.eu/wp-content/uploads/2012/10/2013-11-11-IAB-Europe-OBA-Framework_.pdf

International Chamber of Commerce (2011), Advertising and Marketing Communication Practice Consolidated ICC Code, Document No. 240-46/660 of August 2011, available at: http://www.codescentre.com/media/2083/660%20consolidated%20icc%20code_2011_final%20with%20covers.pdf

Istituto di Autodisciplina Pubblicitaria (2015), Regolamento sulla Pubblicità Comportamentale Online – OBA, November 2015

Iveson, K. (2016), How Pokemon Go will make money from you, The Sydney Morning Herald of 3 August 2016, available at: http://www.smh.com.au/comment/how-pokemon-go-will-make-money-from-you-20160802-gqj457.html

Joung, Y.-J. / Yen, C. / Huang, C.-T. / Huang, Y.-J. (2005), On personal data license design and negotiation, 29th Annual International Computer Software and Applications Conference, 2005. COMPSAC 2005, IEEE

Kanoje, S. / Girase, S. / Mukhopadhyay, D. (2014), User Profiling Trends, Techniques and Applications, International Journal of Advance Foundation and Research in Computer 2014, 1, 1-6, IJAFRC

Kerr, I.R. / Bornfreund, M. (2005), Buddy Bots: How Turing's Fast Friends Are Undermining Consumer Privacy, Presence 2005, 6, 647-655, MIT Press

Kilian, W. (2012), Personal Data: The impact of Emerging Trends in the Information Society. How the marketability of personal data should affect the concept of data protection law, 13(6) Computer und Recht International (Cri) 169

Klein, W.E.J. (2016), Can We Trust For-Profit Corporations to Protect Our Privacy?, September, IEEE Technology and Society Magazine 17

Kopstein, J. (2016), Brands Want To Predict Your Behavior By Mining Your Face From YouTube Videos, Motherboard of 24 May 2016, available at: http://motherboard.vice.com/read/facial-recognition-brands-mattersight

Kroes, N. (2010), Towards more confidence and more value for European Digital Citizens, European Roundtable on the Benefits of Online Advertising for Consumers, Speech of 17 September 2010, available at: http://europa.eu/rapid/press-release_SPEECH-10-452_en.htm

Liem, C. / Petropoulos, G. (2016), The economic value of personal data for online platforms, firms and consumers, Blog post of 14 January 2016, available at: http://bruegel.org/2016/01/the-economic-value-of-personal-data-for-online-platforms-firms-and-consumers

Linkomies, L. (2008), BERR approves of Phorm's targeted-advertising techniques, Privacy Laws & Business United Kingdom Newsletter 2008, 38(Oct), 12

Lomas, N. (2016), WhatsApp to share user data with Facebook for ad targeting — here's how to opt out, TechCrunch of 25 August 2016, available at: https://techcrunch.com/2016/08/25/whatsapp-to-share-user-data-with-facebook-for-ad-targeting-heres-how-to-opt-out/

Marshall, J. (2014), Do Consumers Really Want Targeted Ads?, The Wall Street Journal Blog of 27 April 2014, available at: http://blogs.wsj.com/cmo/2014/04/17/do-consumers-really-want-targeted-ads/

Martens, B. (2016), An economic policy perspective on online platforms, JRC/IPTS Digital Economy Working Paper 2016-05, available at: https://ec.europa.eu/jrc/sites/default/files/JRC101501.pdf

Merikle, P.M. (2000), Subliminal perception, 17, 497, in: E. Kazdin (Ed.), Encyclopedia of Psychology, Oxford University Press

Michael, M.G. (2016), The Paradox of the Uberveillance Equation, IEEE Technology and Society Magazine 2016, September 2016, 14, IEEE

Mik, E. (2016), A Contractual Perspective on Consent and Notification Requirements in Privacy Legislation, Paper presented at the Society of Legal Scholars Conference of 6-9 September 2016, Oxford

Neelam, S. / Sood, S. / Mehmi, S. / Dogra, S. (2015), Artificial intelligence for designing user profiling system for cloud computing security: Experiment, 2015 International Conference on Advances in Computer Engineering and Applications (ICACEA) 2015, 51-58, IEEE

Network Advertising Initiative (2015a), Code of Conduct, May 2015, available at: https://www.networkadvertising.org/sites/default/files/NAI_Code15encr.pdf

Network Advertising Initiative (2015b), Guidance for NAI Members: Use of Non-Cookie Technologies for Interest-Based Advertising Consistent with the NAI principles and Code of Conduct, 18 May 2015, available at: http://www.networkadvertising.org/sites/default/files/NAI_BeyondCookies_NL.pdf

Noto La Diega, G. (2016a), Uber law and awareness by design. An empirical study on online platforms and dehumanised negotiations, 2015/2 European Journal of Consumer Law 383

Noto La Diega, G. (2016b), In light of the ends. Copyright hysteresis and private copy exception after the British Academy of Songwriters, Composers and Authors (BASCA) and others v Secretary of State for Business, Innovation and Skills case, in: C. Franchini (Ed.), Studi giuridici europei 2014, 39-60, Giappichelli

Pandey, K. / Mittal, A. (2016), User profiling on Tumblr through blog posts, 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), 85-89, IEEE

Pang, Y. / Wang, B. / Wu, F. / Chen, G. / Sheng, B. (2015), PROTA: A Privacy-preserving protocol for real-time Targeted Advertising, 2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC) 1-8, IEEE

Pariser, E. (2011), The Filter Bubble: What the Internet Is Hiding from You, Penguin Press

Pittman, A. (2016), The Internet Thinks I'm Still Pregnant, The New York Time of 2 September 2016, available at: http://www.nytimes.com/2016/09/04/fashion/modern-love-pregnancy-miscarriage-app-technology.html

PwC (2015), Global entertainment and media outlook, PricewaterhouseCoopers

Purcell, K. / Brenner, J. / Rainie, L. (2012), Search engine survey 2012, Pew Research Centre Survey of 9 March 2012, available at: http://www.pewinternet.org/2012/03/09/search-engine-use-2012/

Reding, V. (2013), Answer given to the question for written answer E-000850/13 by Mrs Reding on behalf of the Commission, 8 April 2013, European Commission

Reed, C. / Kennedy, E. / Nogueira Silva, S. (2016), Responsibility, Autonomy and Accountability: legal liability for machine learning, Paper presented at the 3rd Annual Symposium of the Microsoft Cloud Computing Research Centre, 8-9 September 2016, Cambridge

Reed, C. (2016), Why Judges Need Jurisprudence in Cyberspace, Paper presented at the Society of Legal Scholars Conference 2016 of 6-9 September 2016

Rottondi, C. / Verticale, G. (2017), A Privacy-Friendly Gaming Framework in Smart Electricity and Water Grids, IEEE Access, 5, 14221-14233.

Rowinski, D. (2011), Mobile Advertising Explosion: Nexage Hits 8 Billion Impressions Per Month, in ReadWrite of 20 August 2011, available at: http://readwrite.com/2011/08/10/mobile-advertising-explosion-n/

Sattler, A. (2018), From Personality to Property? Revisiting the Fundamentals of the Protection of Personal Data, in: M. Bakhoum, B. Conde Gallego, M.-O. Mackenrodt, G. Surblytė-Namavičienė (Eds.), Personal Data in Competition, Consumer Protection and Intellectual Property Law. Springer, Heidelberg

Soltani, A. / Canty, S. / Mayo, Q. / Thomas, L. / Hoofnagle, C.J. (2009), Flash Cookies and Privacy, 10 August 2009, available at: http://ssrn.com/abstract=1446862

Sunstein, C.R. (2007), Republic.com 2.0, Princeton University Press

Surblytė, G. (2015), Competition Law at the Crossroads in the Digital Economy: Is it All About Google? 4 EuCML 170.

Tarabella, M. (2013), Question for written answer E-000850/13 to the Commission, Marc Tarabella (S&D), 28 January 2013, European Commission

Turow, J. / King, J. / Hoofnagle, C.J. / Bleakley, A. / Hennessy, M. (2009), Americans Reject Tailored Advertising and Three Activities that Enable It, Paper of 9 September 2009, available at: http://ssrn.com/abstract=1478214

White, A. / Levring, P. (2016), Facebook Grilled by EU's Vestager Over WhatsApp Merger U-Turn, Bloomberg of 9 September 2016, available at: http://www.bloomberg.com/news/articles/2016-09-09/facebook-grilled-by-eu-s-vestager-over-whatsapp-merger-u-turn

Woodward, J.D. (2000), Is Biometrics an Age Verification Technology?, Santa Monica, RAND

Yan, J. / Shen, D. / Mah, T. / Liu, N. / Chen, Z. / Li, Y. (2011), Behavioral targeted online advertising, in: X.-S. Hua, T. Mei, A. Hanjalic (Eds.), Online multimedia advertising, 213-232, Information Science Reference

Zuiderveen Borgesius, F.J. (2016), Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation, Computer Law & Security Review 2016, 2, 256, Elsevier

Binding Corporate Rules As a New Concept for Data Protection in Data Transfers

Bianka Maksó

Contents

1 Introductory Ideas 502
2 Economic Aspects of Personal Data 503
2.1 Theoretical Background 503
2.2 An Example 504
2.3 Contractual Aspects 506
3 Legal Background of International Data Transfers 508
3.1 Current Rules of the Data Protection Directive 510
3.2 General Data Protection Regulation and International Data Transfer 512
4 Binding Corporate Rules 513
4.1 BCRs as Legal Institution 514
4.2 Content 514
4.3 Authorizing Process 516
5 SWOT of BCRs 518
5.1 About the Method 518
5.2 SWOT Chart 519
5.3 Evaluation 520
6 In Conclusion: Bottom Lines 523
References 524

Abstract It took us only a few decades from the introduction of publicly open and printed telephone-number registers to approach the utopian idea of Laudon's digital information market for personal data. Through the journey concerning data protection we must face challenges in the fields of technological development as well as jurisdictional and legislative issues such as extraterritorial law-making. This paper attempts to provide a brief composition of the economic aspects of personal data given real commercial and strategic value. Additionally, a focus is on conceptual,

Bianka Maksó, dr. jur., is a PhD candidate of the Deák Ferenc Doctoral School of Law, University of Miskolc.

B. Maksó (✉)
Deák Ferenc Doctoral School of Law, University of Miskolc, Miskolc, Hungary
e-mail: jogmakso@uni-miskolc.hu

M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law*, MPI Studies on Intellectual Property and Competition Law 28, https://doi.org/10.1007/978-3-662-57646-5_18

procedural and applicability aspects of a new legal institution called binding corporate rules, which can offer a new approach for companies to ensure an adequate level of protection not only in the cases of data transfer to third countries but also in general business interests.

1 Introductory Ideas

From the time Laudon[1] envisaged a digital market for selling and buying personal data in the era of printed registers, up to our digitalized online world, challenges have been faced in the fields of technological development as well as jurisdictional and legislative issues in data protection like the debated cases of Google Spain and Google[2] or the so-called Safe Harbour decision of Schrems vs. Ireland Data Protection Commissioner.[3] As we are members of a huge digital economy and a vivid information society transferring personal data irrespective of borders or any limitations, being conscious about providing our personal data and controlling our information self-determination, needs real efforts as an important factor of everyday life.

Data is deemed to be the oil of our new age,[4] so the legal environment within which data controllers must conduct themselves must be comprehensive, effective and flexible at the same time, concerning technological development and the needs of rapidly changing international economic and social procedures.

In order to strengthen online privacy rights and boost Europe's digital economy,[5] the new General Data Protection Regulation (GDPR)[6] on 4 May 2016 was published in the EU. It is a part of a comprehensive reform to introduce modernized rules for Member States having the states and private sector entities as data controllers or data processors under its scope as well. Legal harmonization is the pledge of successful cooperation but some experts claim that the rules are considered as extraterritorial legislation, mainly in the field of international data transfer, not because of the scope of the GDPR but because of its effects.[7] Considering personal data as subject to property rights, or moral rights, or as a part of personal identity, or even as trade secrets,[8] undoubtedly gives personal data a high value, so companies must ensure protection both for the rights of data subjects and their own business interests. This entails incorporating privacy protection issues into business profiles,

[1] Laudon (1996), pp. 92-104.

[2] ECJ, Google Spain and Google, C-131/12; ECLI:EU:C:2014:317.

[3] ECJ, Maximillian Schrems v. Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650.

[4] Moorhead (2011).

[5] European Commission (2015).

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ [2016] L 119/1.

[7] Kuner (2015).

[8] Samuelson (2000).

especially in the case of data transfers to third countries. The question of a multinational business is how to cope with this challenge. As private sector entities have borne (some of) the highest risks of data breaches, the tendency of both EU and Hungarian legislation is to give priority to self-regulation.

An adequate level of protection is a key factor of international data transfers. The GDPR, in Article 46(2)(b), enacted binding corporate rules (BCRs) as one of the most important of the legal means providing a guarantee of adequate protection. Article 47 provides detailed rules for the content of BCRs and national laws determine procedural rules for their authorization. The Article 29 Data Protection Working Party has also published several working papers to give guidelines for the creation and application of BCRs. This legal instrument can be deemed as a code of conduct, or a kind of terms and conditions, to effect privacy by design, but so far there have been no convincing arguments, attitudes or practices to demonstrate its legal nature. With just a few available studies in the literature and only a few years of application of BCRs this paper attempts to provide here an academic introduction to the concept and emphasize its advantages as well as its negative features.

2 Economic Aspects of Personal Data

2.1 Theoretical Background[9]

Personality is becoming more and more virtualized[10] as a person is determined by customer codes, e-mail addresses, contract numbers etc. for data controllers. Under this aspect of the seven different types of privacy,[11] this shall be considered as privacy of data (and image). However, neither the people themselves nor their personal data are free goods on the market. On the other hand, many everyday examples destroy this idea, such as direct marketers who buy and sell lists of different personal data sorted by age or preferences.

The concept of the privacy paradox[12] emphasizes that the data subject is sometimes as liable for infringement as the breaching data controller. According to this concept data subjects require protection and lawful use of their personal data without any (financial) investment made by them in advance, but for the promise of the tiniest benefits they are ready to provide as much data as they are asked for. Having this phenomenon in mind, it seems to be more important and more efficient to make the data controller interested in data protection issues than to entitle the data subjects to exercise several rights against the committed infringement.

[9] It is noteworthy that there is still a current scientific debate over the balance of moral rights and interests.

[10] Szabó (2005), pp. 44-54.

[11] Finn / Wright / Friedewald (2013).

[12] Acquisti (2013).

The roots of data protection date back to the 1890s, when S. D. Warren and L. D. Brandeis[13] set the first milestone of the right to privacy as the right to be let alone. The widening of the concept of property to non-material objects led to the conclusion that to the protection of the human body was added a further factor: the protection of personality. Warren and Brandeis were legal pioneers, claiming that a serious need for protection of privacy had arisen which could be deemed as a special method of the protection of property and the execution of the right to property. The subject-matter of protection is the so-called domestic occurrence, the right to be let alone. They determined the general principle of the aim of privacy protection, and this can be personalized to each person. They also pointed out the distinction between public figures and non-public figures, concluding that the former waived part of their rights to be let alone. Public figures live in the eyes of the public, which necessarily means the publication of several pieces of personal data. This is the first appearance—and the starting point—of informational self-determination.

2.2 An Example

In order to apply Luhmann's theory[14] to data protection issues, the following hypothetical example of data protection could be examined: the data subject requires that the data controller collect and process data according to the purpose determined in advance for the determined period of time with the informed consent of the data subject. Requirements assume the possibility of delusion. In this example delusion is the fact of infringement and the occurrence of personal data breach. Then the right for enforcement and the claim for compensation become the new requirements of the data subject. These are normative samples given by law as a reaction of (un) fulfilled requirements.

The demands or economic maintenance of a profit-oriented business often break the above- detailed requirements. The data controller would like to process our personal data as long as he benefits from them by profiling persons, or even selling data for profit, but all of these activities are prohibited by (mostly national) laws. So in many cases the rules declared by law are not in line with economic rationalism.

Another attitude towards the real value of personal data is given by Posner. According to his theory of maximizing well-being, the function of legal rules is to ensure the biggest possible happiness for most of the members of the whole society. However, economic procedures consist of opposing interests. Market participants should make a cost-benefit analysis before making decisions.[15] Assume that the price of an item is 80 units. A purchaser who is committed to data protection would buy it for 100. If Purchaser had any concern about data protection during the

[13] Warren / Brandeis (1890).

[14] Luhmann (1979); For further interpretation see: Csegődi, T. L. (1979): A jog pozitivitása mint a modern társadalom feltétele, in: Jog és szociológia., pp. 123-142., Válogatott tanulmányok KJK.

[15] Posner (2011); or Tóth (2004).

transaction, he would surely cancel the contract, but he would pay 105 for the item if Seller applied data protection measures.[16] These measures cost 15 units for Seller. So the transaction could be realized in the following ways:

(A) Seller does not apply data protection measures, this is noticed by Purchaser. The Purchaser will not buy the product, and will save 105 units. Seller will not get 80 as he wanted and in the long term Purchaser is not going to use his service.
(B) Seller does not apply data protection measures, but this is not noticed by Purchaser, so the transaction will be fulfilled at the price of 90, when the profit of Seller is added. Both parties are satisfied in the short term. In the long term Seller is able to use or even sell for profit the personal data of Purchaser, who can easily become vulnerable to data controllers. If the infringement is noticed, Purchaser may bring a lawsuit against Seller.
(C) Seller applies data protection measures for 15, then the price of the item is increased (90 + 15) to 105. The Purchaser will buy the product and both of the parties will be satisfied in the short term. Purchaser will buy from Seller in the future as well, preferring his data protection measures, so this is a good transaction in the long term as well. People tend to choose what they prefer from among the readily available options. In this example Purchaser will get the product and be ensured that his personal data are protected. Seller increases his costs, leading to higher prices, but he is able to attract and keep new partners. This complex system benefits the whole society, so it can be deemed as Pareto-efficient: either the status of both parties becomes better or only one improves but the other does not become any worse.

Besides profitable aims, alternative factors also influence profit-orientated entities: moral and social norms, the hope of future and recurrent transactions, the durability of the current contract, and last but not least their reputation in the market. Then a method of price discrimination is applicable to keep the market entities competitive and able to keep their customers. The above example is simplified but good enough to demonstrate the importance of the role of data protection measures. Additionally, the high risk of data thefts and damages deriving from that for which the data controller may also be liable in case of applying poor data security measures has not been taken into consideration and fines imposed as a result of an administrative procedure have not been added either.

In conclusion, it is found that applying data protection measures will be more profitable than avoiding them, in the long run.

According to Laudon's theory, the key to solving data protection issues is not creating obligatory rules or establishing institutions for supervising, but maintaining a strong digital market for personal data.[17] In this market the interests of the data

[16] An American would pay 50 cents more for a good which is provided by a business which applies data protection measures; Acquisti (2013).

[17] Critics say that this would lead to a world in which there is no privacy at all and discrimination would aggravate the gap between rich and poor people.

subject and the data controllers would be balanced in line with making profit out of the data.[18] Every data subject would have his own account with which he would be able to sell his personal data at a price he or his agent negotiated with the buyer. The data subject would be able to follow the data he sold and would get a certain per cent of profit from further transactions made by the buyer with his data. In such a market, legal rules are only tools with which to satisfy a need of the society. But as is explained above, legal rules are not always suitable for this purpose. The legal and the economic nature of obligatory rules have to be as closely aligned as possible. One potential way to achieve this is to create rules for self-regulation.

Self-regulation is becoming more and more popular among business entities as the tendency of legislation in many Member States of the EU supports this type of regulation. During self-regulation rules and guarantees declared by law are shaped by companies as they best fit their activities, while keeping an obligatory and lawful nature to make them applicable to real-life situations. One such option would be the application of BCRs that provide specific rules of a binding nature fit for the company without the act of the legislature but with the necessary authorization of the national data protection authority (DPA), and ensuring the right to judicial remedy for the data subject.

2.3 Contractual Aspects

In this part of the paper it will be looked at what the *de facto* uses of personal data mean in theoretical economics terms, i.e. as a commodity. According to Posner,[19] privacy is one of the consumer goods and as such is a valuable product. He built up a theoretical construction between personal data and commerce: people sell themselves, for example at a job interview, as commercial goods. If they do not provide all personal information relevant in the certain situation, they can hide the real—disfavoured—factors and qualities to mislead the other party. In conclusion, he strongly disapproves of a law which allows the entitled to hide—or in other words protect—personal data as it results in distorting the market and real competition. However, he admitted that the person could only save himself from a disadvantageous transaction if he was entitled to retain personal information and others were prohibited from seeking sensitive data or keeping someone under surveillance. The importance of this entitlement is reflected in the latest survey of the EU on data protection,[20] according to which people complained most about online service providers and telemarketers. As a mention that in everyday life people do not seem to be conscious about these fears as the application of online services and the amount of personal data provided is growing each day. According to the EU survey, people deem their data on financial and health issues the most sensitive, followed by their address and

[18] Laudon (1996), pp. 92-104.

[19] Posner (1978).

[20] European Commission (2011).

fingerprint. However, for the business sector it is not the financial data, but data on our interests, that have high priority, in order to be able to offer services that best fit consumers.

A good example is the online mailing system, in which the metadata and the full content are available for the provider. The only thing to deliberate is whether the mailing service is worth enough to us in exchange for the data. According to Posner,[21] privacy as a sum of personal data is an intermediate rather than a final good, as people can utilize their data to achieve or get something, e.g. consumer data become a natural intermediate good in case of a simple purchase transaction.[22]

It is generally thought that privacy and data protection are equal to the right to be alone. That is the reason why the majority of infringements remain latent, as the data subject does not raise a claim because of the unlawful activity, i.e. the unreasonable and causeless disturbance, until it has (financial) malware results. A common example of causeless disturbance is the spread of spam mails by sellers. If Seller knew the real needs and preferences of the Purchaser then the transaction would become easier to manage, which derives from the basic principle of the methods of economy, according to which the demand assumes the supply. If Seller knew precisely what Purchaser really wanted and how much money he was ready to pay for it then the costs of transaction would be reduced by the costs of contracting, bargaining and other negotiations.[23] The Purchaser also has an advantage, as he can avoid the necessary costs and losses deriving from market research. This would help in personalizing services, planning trends and needs and maximizing the efficiency of marketing costs while minimalizing the risk of transaction. However, it would be seriously disadvantageous if Seller were to know certain information that Purchaser would not choose to release because of its sensitivity. In the case of a negotiation for a life insurance contract, the more sensitive the personal data is, the more potential for harm it has, which deeply influences the final details of the contract. Finally, most privacy problems occur because there are differences between the parties in respect to the available information and this causes informational asymmetry, which can easily result in privacy infringement and market distortion.

However, according to Varian[24] certain elements of privacy rights can be subject to a contract, e.g. the right to process certain personal data can be leased for a certain purpose for a certain period of time with the informed consent of the data subject. The next questions to answer are whether lists of these data can be deemed the intellectual property of the creator of the lists and whether these lists can be subject to further sales contract or lease agreement. If the answer to both questions is in affirmative, the right of the data subject to informational self-determination should be taken into account as well. This process would create a secondary market in which the goods are the personal data and the use of them creates profit. However, in the long term the profit would go not to the data subject, who is ideally entitled to

[21] Posner (1978).

[22] Huang (1998).

[23] Huang (1998).

[24] Varian (1996).

determine that use, but to the data controller, who really determines it. In the short term the data subject can achieve some additional benefit, e.g. an e-mail account free of charge, but in the long term most of the time he becomes vulnerable and loses the opportunity to determine the use of his personal data. This kind of loss is deemed subjective harm[25] if the data subject has the feeling of surveillance by the 'little brothers' of the market.

In our digital age the 'little brothers' of the market cannot be limited by technological factors or state borders. As digitalization is the pledge of growth, the European Union has promoted it with several efforts to modernize the single market to make it fit for the new challenges and needs. One of the main objectives of the process is to provide an up-to-date legal framework to ensure that personal data enjoy a high standard of protection everywhere in the EU[26] and EU citizens as data subjects are entitled to adequate levels of protection outside the jurisdiction of the EU.[27] This two-pillar-structure consists of rules not only for electronic communications and services but also a comprehensive normative background on the collection, control, process and transfer of personal data with several rights to remedy in case of infringement.

3 Legal Background of International Data Transfers

The European Union, originally an integration for economic cooperation, has tended to establish a general and extensive legal environment in many fields of integration. In the early 1990s it became essential to create the next generation of data protection regulation. Besides the paper-based state registers, data controllers of the private sector and automatized data processing also necessitated the modification of the laws in effect. This development process is testified to by the fact that the issue of privacy and data protection was raised to the level of primary law by the approval of the Treaty of Lisbon[28] and the Charter of Fundamental Rights of the European Union.[29] In the field of data protection EU regulation was separated into four different sectors[30]: general data protection, data protection in relation to EU institutions, data protection in the electronic sector and last but not least other sectorial protection, e.g. criminal data or environmental data. Nowadays these sectors are being developed, but the emphasis has been put on the electronic issues. The creation of the legal frames of protection of personal data began with the approval of the Data

[25] Acquisti (2010).

[26] European Commission (2016).

[27] Note: with reference to data protection, 'EU' stands for the European Economic Area (EEA).

[28] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, OJ [2007] C 306/1.

[29] Charter of Fundamental Rights of the European Union, OJ [2016] C 202/389.

[30] Oros / Szurday (2003).

Protection Directive[31] in 1995. Member States were allowed a period of 3 years from its entry into force to transpose its rules into national measures.[32] Currently the Directive is binding in 28 Member States and the three EEA countries. As the Directive left only a narrow margin to the Member States for manoeuvring, the style of harmonization can be considered as total. However, as a result, not common but 28 different data protection regulation regime exists.

The reform procedure initiated in 2012 has brought major changes, in line with the demands of data subjects and data controllers. The approval of Directive 2016/680[33] and the GDPR has had significant consequences, although the GDPR has entered into force on 24 May 2016 and will apply from 25 May 2018. Regulations are legislative instruments of general and direct application with binding force on Member States though without the requirement of transposition into any national legislative measure. Two main consequences will arise from the nature of this legislation: (1) Member States will have no power to apply regulations incompletely or transpose rules into their national legal system in the field in question, and (2) the Member States waive a part of their law-making sovereignty, so that legislative actions will necessarily be annulled. At the same time, the obligation of legal development will be imposed on the EU law makers, which is a tough challenge concerning the rapid improvement of technology, for example in the field of data transfer and the spread of WEB2 solutions.

In this paper the rules of international data transfer are discussed, as multinational companies with affiliates in third countries and a registered office in the EU have to comply with these regulations if they act as data controllers of the personal data of EU citizens. However, current rules do not define the concept of "transfer to a third country". Furthermore, uploading data to a website is tantamount to the subsequent transmission of data to anyone who connects to the internet from anywhere in the world, since the information in question is not sent automatically to people, so that uploading was not considered to be data transfer to a third country.[34]

According to the latest Eurostat survey, conducted in spring 2015, 81% of the participants answered that enjoying the same rights and protection is important for them regardless of the jurisdiction under which the data controller processes their personal data.[35] EU legislators have to take these needs into serious consideration in

[31] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OL [1995] L 281/31.

[32] Ibid., Article 32(1).

[33] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ [2016] L 119/89.

[34] ECJ, Criminal proceedings against Bodil Lindqvist, C-101/01, ECLI:EU:C:2003:596, paras 56, 59, 60, 70.

[35] Special Eurobarometer 431 / Wave EB83.1: Data protection, Fieldwork: March 2015, Publication: June 2015 http://ec.europa.eu/public_opinion/archives/eb_special_439_420_en.htm#431.

order to create a satisfactory legal framework ensuring the fundamental right of protection of personal data and privacy for EU citizens. It is hard work, considering that personal data used in virtual and economic processes cannot be stopped at the geographical or jurisdictional border of the EU Member States. That is why some experts and leading scholars argue that the Directive has, and the GDPR will surely have, an extraterritorial nature and effect, as data controllers must obey the rules for an adequate level of protection in third countries as well, irrespective of territorial jurisdiction or their personal law in cases when they control the data of EU citizens. However, if the data controllers have no establishment or assets in, or other links with, the EU, enforcement is difficult.[36]

3.1 Current Rules of the Data Protection Directive

The rules of international data transfer can be separated into three major topics. Firstly, there is a default rule declared by Article 25 according to which personal data is only allowed to be transferred if the third country in question ensures an adequate level of protection. Paragraph (2) of the same Article provides details defining adequacy. The European Commission is entitled to enter into negotiations with the country in question to remedy the situation. The Commission also has the right to determine in a formal decision whether a third country ensures the adequate level of protection. According to Article 25(6), the Commission may find that a third country[37] provides the adequate level of protection by its domestic law or international agreement in effect. Secondly, the derogation of the default rule enacted in Article 26 with regard to personal data is allowed to be transferred to third countries which do not provide adequate protection in six different situations. Thirdly, Article 26(2) creates a solution for data transfers to third countries without adequate levels of protection as the data controller can adduce adequate safeguards.

According to the rules detailed above the key factor is the adequate level of protection. Neither the concept nor the content of it are determined in the Directive. The level of protection afforded by a third country is to be assessed in the light of all the circumstances surrounding a data transfer, with particular consideration given to: the nature of the data; the purpose and duration of the proposed processing operations; the country of origin and the country of final destination; general and sectorial rule of law in force in the third country in question and security measures which are complied with in that country.

Only case law[38] gives viewpoints according to which adequate level of protection 'signifies that a third country cannot be required to ensure a level of protection

[36] Ryngaert (2015).

[37] List of countries can be found here: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/. Note: Hungary was declared among these countries before its accession to the EU.

[38] ECJ, Maximillian Schrems v. Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650, para 73.

identical to that guaranteed in the EU legal order' but it 'must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection'. This means that the level can differ but must be effective in practice in order to ensure a high level of protection essentially equivalent to the standard guaranteed within the EU. As for case law, in Maximillian Schrems v Data Protection Commissioner,[39] the safe-harbour mechanism was found not to be able to provide an adequate level of protection in the USA. Among other reasons the lack of an independent supervisory authority, guarantees enacted by law and enforcement procedures, as well as the unsuitable behaviour of data controllers, led to this conclusion. The European Commission concluded the approval process and as its result the so-called Privacy Shield has been introduced to ensure an adequate level of protection in the case of data transfers to the USA. Although in this case an agreement, which is claimed rather a political and not a legal one, was quickly reached between EU and US negotiators. The result is the text of 'Commission Implementing Decision of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield'. For the multinational companies and data processors with transatlantic affiliates as a suitable, long lasting and applicable legal tool would be a BCR. However, many companies deem the self-certification burdensome and the effectiveness of it is still questionable, so it will be reviewed, hopefully with a strong consideration of the applicability of the GDPR, by the EU Commission in the autumn of 2017.

In most cases data controllers apply appropriate contractual clauses. Standard clauses are approved by the Commission,[40] whereas ad hoc clauses must be pre-approved by national DPAs for the transfers to legalize the guarantee of an adequate level of protection. This method can hardly be applied in cases of regularly recurring transfers including huge amounts of data.

More important is the third way of ensuring the adequate level: by self-regulation, specifically, applying binding corporate rules. This legal means is not enacted literally in the Directive and few Member States[41] recognize it as a legal basis for third-country transfers.[42] It is noteworthy that, although in the USA self-regulation

[39] ECJ, Maximillian Schrems v. Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650, para 29.

[40] 2001/497/EC: Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (Text with EEA relevance) OJ [2001] L 181/19; 2004/915/EC: Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries OJ [2004] L 385/74; 2010/87/EC Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council OJ [2010] L 39/5.

[41] See for details: Article 29 Data Protection Working Party: National filing requirements for controller BCR ("BCR-C"), available at: http://ec.europa.eu/justice/data-protection/international-transfers/files/table_nat_admin_req_en.pdf.

[42] Note: the legal basis of BCRs came into effect on 1 Oct 2015 in Hungary.

started in the early 1990s, it has not had a successful history. It was rather promoted than applied, since a well-detailed self-regulatory method including audits and certifications is deemed mostly a burden for its subjects.[43]

3.2 General Data Protection Regulation and International Data Transfer

In its Recital (101), the GDPR emphasizes that data transfers are necessary for the expansion of international trade and international cooperation, which raise needs and requirements to be coped with. GDPR retains the major conceptual structure and rules of international data transfer, including the factor of appropriate safeguards for the data subjects, in order to ensure the protection of fundamental rights of EU citizens and every data subject who are subject to the GDPR. In Article 49 GDPR introduces a new derogation according to which a transfer may take place with the notification to the national DPA if is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances. This rule derives from the demands of legitimate interests of companies but because of its complex nature it may be of 'limited use in practice' according to practitioners.[44] It expands its territorial scope—or at least its impact—outside the EU by Article 3, which declares its scope on the processing of personal data of data subjects who are in the Union by a controller or processor not established in the EU. Article 15(2) emphasizes that the data subject has the right to be informed of the appropriate safeguards in the case of data transfers to third countries. Furthermore, the data controller is obliged to record several details on data transfers to third countries according to Article 30.

As a novum, the GDPR differentiates between the third country, a territory or a specified sector within a third country in respect of adequate protection. Replacing the term of adequate level of protection, such safeguards under the Directive and the GDPR are to be recognized as guarantees that are not already ensured in the targeted country. In the case of adequacy decisions, which still comprise an important method, in Recital (104) it defines the features assessed to evaluate adequate protection: the respect of the rule of law, access to justice as well as international human rights norms and standards, and general and sectoral law, in which the third country must ensure sufficient guarantees essentially equivalent to that ensured within the EU. The GDPR also states (in Article 45) that adequacy will be reviewed at least every 4 years. The legal basis of adequacy regarding data transfer is exhaustively declared, including adequacy decisions of the Commission and other

[43] Wright / de Hert (2016).

[44] http://privacylawblog.fieldfisher.com/2016/getting-to-know-the-gdpr-part-9-data-transfer-restrictions-are-here-to-stay-but-so-are-bcr/.

appropriate safeguards listed in Article 46, including standard data-protection clauses, an approved code of conduct or an approved certification mechanism.

As a milestone in legislation, BCRs have been declared by the legislature the most important safeguard among private sector entities and the second one in general, pursuant to Article 46(2). Article 47 provides the conceptual and partly procedural, but mostly minimum substantive issues of BCRs, which result in their official recognition. Besides these normative rules, the Article 29 Working Party has released several working papers[45] to support national DPAs and BCRs applicants as well, considering that BCRs have to be approved by the competent national authority. Conclusively, with this enactment GDPR removes further obligation of any data processor to obtain additional approval in advance from data protection authorities to transfer data to third countries.[46]

Other mechanisms are also introduced among the adequate safeguards in Article 46, like legally binding and enforceable instruments between public authorities or bodies; standard data-protection clauses adopted by the Commission or the national DPAs; an approved code of conduct; and an approved certification mechanism. As for the latter, two stipulate that transfers must be conducted on the basis of binding and enforceable commitments.

4 Binding Corporate Rules

The primary aim of BCRs is to voluntarily create a single but complex system of rules, i.e. a compliance framework which results in a code of conduct or a set of terms and conditions at a multinational company to comply with the legal requirements of international data transfers to ensure an adequate level of protection in third countries. BCRs are designed for companies to provide legal grounds for international data transfers among the members of their group of companies in third countries. The concept 'corporate group' may vary from one country to another, but the principle behind this concept must be interpreted based upon the fact that these companies are usually set up under the responsibility of a headquarter. GDPR in Article 4(19) solve this difficulty as determines the concept of the group of undertakings.

In the first years of its appearance BCRs were not considered 'the only or the best tool for carrying out international transfers but only as an additional one',[47] and it was also argued about its effectiveness, claiming that BCRs, lacking enforceable

[45] In connection with BCRs the relevant working papers are the following: WP 74, WP 108, WP 153, WP 154, WP 155, WP 176, WP 195, WP 204.

[46] Directive 95/46/EC Article 19 point e) declares that proposed transfers of data to third countries may be subject to notification in advance for the national DPA.

[47] Article 29 Data Protection Working Party: (2003) Working Document: Transfers of personal data to third countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp74_en.pdf.

and effective rules, were just 'paper tigers'.[48] Nowadays, however, the application of BCRs is spreading. According to official publications the number of multinational companies using BCRs is slowly growing.[49] Furthermore, the GDPR, reflecting the world-wide tendency of data protection, also supports co- and self-regulation, in which BCRs are in a privileged position. For instance, in Hungary, within a period of only 1 year after the enactment of BCRs, 18 holdings of multinational companies, including more than forty independent companies, have completed the authorization procedure.[50]

4.1 BCRs as Legal Institution

Pursuant to Recital (101) of the GDPR, BCRs include all essential principles and enforceable rights to ensure appropriate safeguards. Article 4(20) of the GDPR contains a normative definition according to which BCRs mean personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity. The recital defines it as a sum of principles and rights but the normative text of the GDPR determines it as policies, which is an insupportable difference.

4.2 Content[51]

4.2.1 Binding Nature

Pursuant to GDPR Article 47, BCRs shall be legally binding and apply to and be enforced by every member concerned of the group of undertakings by a clear duty for all the members. Internal rules declared in the BCRs of a corporate group cannot replace normative obligations that are binding by law, but only their obligatory nature can make it sufficient to ensure protection. Binding force has two aspects: one is internal, the other external. Internal binding force implies that the members of the corporate group, as well as each employee within it, must comply with the rules of the BCRs, so the rules have to be clear enough to be followed and sanctions must be available in case of a breach of the rules. Internal binding force can be incorporated by intra-group agreements or internal collective agreements; sanctions such as

[48] Baker (2006).

[49] List of companies, for which the EU BCR cooperation procedure is closed, available at: http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm.

[50] List of companies available at: https://www.oecd.org/sti/ieconomy/46968784.pdf.

[51] For further substantive issues see: WP74 and WP 153.

salary cuts or termination of employment may strengthen obedience. External binding force means that data subjects under the scope of BCRs must become third-party beneficiaries and must be entitled to enforce compliance before the competent data-protection authority and/or court to claim for remedy. Nevertheless, unilateral declarations cannot be regarded as a legal basis of third party beneficiary rights for individuals in all states. This enforceability, however, does not annul the right of the data subject to lodge a complaint before the national DPA or courts because of legal infringement ensured by law. BCRs must emphasize their legally binding nature. For example, the BCRs of a well-known IT company include the declaration that this is a 'binding agreement' with which all affiliated companies 'must comply'.[52]

4.2.2 Content of Expressly Conferred Enforceable Rights and Other Elements

Pursuant to GDPR Article 47(2) multinational companies must specify at least the following details in BCRs. BCRs have to overcome the level of abstraction of legislation and have a practical fit with the transferring and data-processing transactions. Details and the level of abstraction have to be sufficient to allow DPAs and the data subjects to assess and evaluate that the transfer to third countries is adequate.

BCRs must include the structure and contact details of the group of undertakings and many details of the transaction of data transfers or set of transfers. This characteristic of BCRs provides the opportunity for companies to create rules which are tailored to their needs and requirements. They can determine the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country. As these elements will differ for each company, it makes each set of BCRs unique.

BCRs must give priority to the application of the general data-protection principles such as purpose limitation, legal basis for processing, the rights of data subjects including at least the right to object, right to obtain data, the entitlement to lodge a complaint and to claim for redress and compensation. For instance, the BCRs[53] of an online service company list several general and specific principles and declare the entitlement to observe while another BCRs differentiate into four different groups the rights ensured to the data subject.

As a general requirement, in BCRs an internal complaint-handling process must be set up for complaint procedures to enforce the granted rights of the data subject. In one such procedure, the complaint is directed to Customer Support—a clearly identified department, as is required in WP 153—which shall investigate and attempt to resolve concerns at first instance. A guarantee for the data subject is that a European member of the multinational company has to accept responsibility for and

[52] Hewlett Packard's BCRs are available at: http://www8.hp.com/uk/en/binding-corporate-rules.html.

[53] eBay's BCRs are available at: http://www.ebayprivacycenter.com/sites/default/files/user_corporate_rules_11-2-09_v1-01.pdf.

agree to take the necessary action to remedy the acts of other members of the corporate group in third countries and to pay compensation. However, DPAs can accept the liability mechanisms on a case-by-case basis. The burden of proof is also placed upon this member, which in a lawsuit or in an administrative procedure can prove that the member of the corporate group in the third country is not responsible.

As transparency is necessary to demonstrate that data subjects are made aware of the details of data processing and transfer, it is important to include rules about the mechanism for recording and reporting to the competent DPA and informing the data subject. Practically, companies should make their BCRs publicly accessible for data subjects. National DPAs should also support transparency by releasing the list of companies using authorized BCRs. However, it must be noted that in a well-structured set of BCRs trade secrets, know-how and data of business interest can be released, so its publicity has to be interpreted wisely. It must be highlighted at this point, that the core text of published BCRs are usually less detailed and more general than the documentation submitted for the DPAs for authorization.

In BCRs companies have to create rules for the cooperation mechanism with the supervisory authority as well, as one rule makes a commitment of diligent and appropriate response toward DPAs. BCRs regulate the tasks of the data-protection officer in charge of the monitoring-compliance mechanism ensuring the verification of compliance. BCRs must create a duty for the group to have data-protection audits on a regular basis, take corrective actions, provide appropriate data-protection training to personnel and report changes.

If the economic factors of a company change, BCRs need to be adapted to such changes. This is a big advantage of BCRs: they can be tailored to the needs of the company in any situation. In the case of updates new members have to make a clear commitment to be effectively bound by the rules and other changing details have to be determined, but the general principles, the ensured rights and the level of protection guaranteed by the original BCRs cannot be reduced.

As for the extraterritorial impact of this legal means, jurisdictional issues may arise. To avoid arguments, it is useful to specify the relationship between the BCRs and the relevant applicable law, as the Article 29 Working Party emphasizes in WP 153. One situation is interesting: when the local law in the third country requires a higher level of protection for personal data—or impose other obligations on data controllers -, it will take precedence over the BCRs.[54]

4.3 Authorizing Process

According to GDPR Article 47(1), BCRs shall be approved by the competent national DPAs. The participation of national DPAs is entirely voluntary[55] but in many Member States BCRs are only applicable if the approval of the national DPA

[54] WP 153 point 6.4.

[55] WP 108.

is available. It is noteworthy that this procedure can be deemed as a general administrative procedure that results in approval, but an expert says that these procedures have to be concluded according to the own rules of the national DPAs, as in Hungary does.[56]

The procedure of the lead authority is quite complex and can take up to a year, but generally runs from one to six months.[57] A schematic procedure would start with the submission of the application form of the company to the lead DPA providing several types of information such as contact details, information to justify the choice of DPA, the basic structure of the company, the details of the processing activities including the origin and the targeted country, the purpose and the means of the processing, information summarizing how the required elements of WP74 are fulfilled, information about internal adoption and the details of enforcement of the binding nature. The draft of the BCRs is also a compulsory annex of the application. Commercially sensitive information or trade secrets have to be indicated in advance. Additional information and the details of the authorization process, being a classical public administrative procedure, may vary according to national laws. The lead DPA is obliged to examine the application and transmit all the data to other relevant DPAs.

During this process effective cooperation between the applicant company and the lead DPA is essentially a key factor determining the length of the procedure. The draft BCRs are examined by the lead authority and each relevant DPA has the right to make comments and propose further requirements to comply with their national laws. To reach full compliance these comments and requirements have to be adopted into the final BCRs, so the applicant may have to make modifications to the draft several times, as the lead authority informs the applicant of the result of the other DPAs' evaluation. This part of the process may take a long time, which is a drawback of the procedure. For instance, the Hungarian DPA acts in three different procedural roles: it can act as (i) the lead authority to the first introduction of a new set of BCRs,[58] (ii) a relevant authority in the authorization process of a new set of BCRs or (iii) the DPA which authorizes those BCRs which have been already in effect and which have started to applied in the domestic country.

In order to facilitate harmonizing the legal background for the usage of BCRs, a mutual recognition procedure has been introduced. Within this cooperation, once the lead authority (which is chosen by deliberating on different factors like the country of the registered office of operational headquarters of a group or the location of the company within the group with delegated data-protection responsibilities or the location where the decisions are made on data transfers or the location from

[56] Horváth-Egri Katalin (2015). However, it is noteworthy that according to the draft modification of Hungarian Data Protection Act the authorizing process will be administered according to the rules of the general administrative procedure.

[57] See the country-specific details in the table, available at: http://ec.europa.eu/justice/data-protection/international-transfers/files/table_nat_admin_req_en.pdf.

[58] Until October 2017 the Hungarian DPA has not act as lead authority.

the data is collected[59]) finds that BCRs meet all the requirements set out in national and EU law, also taking the working papers into consideration, the DPAs within mutual recognition accept this as sufficient basis for authorization without any further requirements[60] created to demonstrate a simplified authorization process. In addition, in some cases, such as that of Hungary, some Member States do not take part in the mutual recognition procedure but the relevant authorities concerned take part in the co-operation procedure created by the Article 29 Working Party in WP108, which has the same result.

The fee of the procedure also varies in each country. The Hungarian price is deemed to be relatively high at HUF 266.000 (EUR 864.38[61]). In Denmark the procedure is free of charge, in Malta an annual fee has to be paid regarding the updates of BCRs and in Cyprus it costs EUR 42.50, while in Slovenia EUR 22.66 must be paid.[62] Nonetheless many companies reject the idea of BCRs, since the unrealistically high costs of the facilitating law firms and advocates during the drafting period and the administrative procedure hardly show a satisfactory return. In comparison, the US companies in case of self-certification under Privacy Shield have to pay a fee based on their total revenue, but usually are less than $1000.[63]

Finally, the totally compliant BCRs will obtain approval and then act as a legal basis for data transfer to third countries. The national DPA registers the company and informs the European Commission of the approval.

5 SWOT of BCRs

5.1 About the Method

Applying BCRs is a means of self-regulation. The measure of independence during self-regulation depends on the intervention of legal rules. In the case of BCRs there is a deep and strict intervention: as legislative acts rule this field of law at national and at EU level, there is a continuous authoritative control and cooperation during its creation. However, there is little experience in the judicial remedy deriving from the infringement of BCRs. Self-regulation cannot substitute for legal rules but it is suitable for grounding normative and mainly executive rules which fit into the

[59] See the full list of factors in WP 108 point 3.3.

[60] So far 21 countries take part in this process. See the list: http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/mutual_recognition/index_en.htm.

[61] Currency rate available at: https://www.mnb.hu/arfolyamok.

[62] http://ec.europa.eu/justice/data-protection/international-transfers/files/table_nat_admin_req_en.pdf.

[63] https://www.lexology.com/library/detail.aspx?g=7a63e6fe-e1f8-4a17-a517-77ee1c0f4218.

current technological, economic and social status and are suited for the plans and aims of a particular entity. These methods combine the functions of a legislature and a self-compliance check mechanism as well.[64] The abbreviation SWOT covers the method of strategic planning common at EU level.[65] With this analysis the strengths, weaknesses, opportunities and threats of BCRs can be highlighted. Strengths are supportable internal factors that can be developed for increased benefits. Weaknesses are internal factors to be revised or converted to have a final positive effect. Opportunities and threats are both external factors on which the examiner cannot have an impact. Benefits can be achieved by developing the opportunities. Threats should be attempted to avoid or lower the risks of their occurrence.

5.2 SWOT Chart

S—Strengths	W—Weaknesses
– Based on expertise of the field of the certain industrial sector or company, the company's needs and features can be taken into consideration – more determined willingness to obey – opportunity to solve problems in house as rules serve the company in line with the data subject's rights – harmonizes the data-protection policy among the members of the multinational company – transparency of the collection, processing and transfer of personal data will develop – data-protection policy will be integrated into business operations – increased flexibility and accountability – export of the EU data-protection policy – no need for authorization of data transfer in advance – no need for contractual agreements of data transfer in advance	– Limitation of the data subject's informational self-determination – generalization of the standard of protection – not clearly determined group of those applying it: companies and/or legal entities like NGOs, foundations, associations – (can be) incompatible with local laws, mainly in third countries – need for substantive and procedural legal environment in all of the Member States of the EU – time-consuming administrative procedure to have it authorized – the more countries involved, the harder authorization becomes: not efficient for smaller companies – binding only for the multinational company, not for the country or a territory or specified sector or the partner as sub-data processors – no clear method of enforcement so far – may negatively influence competition

(continued)

[64] Szőke (2015).

[65] An example of its application is listed in Article 27 of Council Regulation (EC) No 1083/2006 of 11 July 2006 laying down general provisions on the European Regional Development Fund, the European Social Fund and the Cohesion Fund and repealing Regulation (EC) No 1260/1999, OJ [2006] L 210/25 (no longer in force).

O—Opportunities	T—Threats
– Development, profit (over time) and the trust of the data subjects – EU compliance – applicable to companies whose members are in bench structure – applicable to specified sectors – improved relationship with the DPA – better PR for the company – mutual recognition among states – need for new statutory regulation – need of new services for drafting BCR	– Binding force (internally and externally)? – updates? – changes in structural features of the company? – changes in legal environment? – forum shopping? – sub-data processor outside the company group ? – jurisdiction, power, competence?

5.3 Evaluation

5.3.1 Strengths

The most important advantage of applying BCRs is that the data-protection policy will be integrated into business operations. Once it is authorized and implemented among the members of the multinational company, its application can decrease further administrative burden in connection with data transfers as it substitutes contracts and the approval of the transfer by the national DPA in advance necessary for every transfer transaction. BCRs can be created for the organizational or operational needs of the company, which concludes the avoidance of the conflicts of the application of variable national laws on data transfers. Their application also ensures flexible and suitable rules while the level of obedience can remain high. In one document all kinds of rules of data protection can be stated and the remedies can be declared as well. In addition, a member of the corporate group has to be marked as the firm which will bear the responsibility in case of data protection breaches and incidents.

If EU standards, incorporated in BCRs, are applied in companies which are not subject to the EU law in third countries—as they are members of a multinational company—the European high-standard privacy policy may be exported. The same rules of data protection will then be followed in all affiliates all around the world irrespective of national laws and jurisdiction.

There will be no need for authorization of each data transfer in advance by national DPAs. There will be no need for contractual agreements on each data transfer in advance among firms or even with the employees. BCRs are a kind of a preauthorizing of all data transfers which are exercised under these rules.

An in-house complaint handling and problem solving process has to be established which can be an additional and hopefully faster and easier way of solving data breaches out of court between the data subject and the data controller. It can be also a serious motivation on the side of the data controller for compliance and enforcing binding BCRs internally.

5.3.2 Weaknesses

BCRs constitute a limitation of the data subject's informational self-determination. An employee or a customer will become subject to these rules automatically and there will be no real informed consent to data processes and transfers, as the data subject gives his or her consent for further data transfers in advance.

BCRs generalize data-protection rules irrespective of the nature of the third country of a given data controller or even a given data subject or the nature and details of the transfer or the data, which is a serious drawback.

Literally speaking, only companies are entitled to be subject to BCRs, as the laws in effect and the GDPR use the word 'undertaking'—in many of the official languages of the EU—but national laws sometimes include corporations and other legal entities, like NGOs, foundations or associations which causes difficulty in interpretation and application. However, the GDPR expands the scope of BCRs to groups of enterprises engaged in a joint economic activity. Also GDPR defines the concept of group of undertakings in Article 4 (19) as a controlling undertaking and its controlled undertakings, which concept fits well to the idea of a BCR-ruled data protection policy.

The most deceptive disadvantage of BCRs is that they serve as guarantee only for the company and its affiliates, not for all the data-protection incidents in the (third) countries. Considering this fact, the data processor or sub-processor in a third country is not obliged to fulfil the requirements of the relevant BCRs, so the level of protection can be damaged or violated easily; however, the liability still lies on the shoulders of the data controller in the EU.

In some countries[66] the substantive and/or procedural rules for BCRs do not exist yet, and national laws are inapplicable. It may easily happen that an authorized BCR may not be deemed as a suitable legal tool in another country to justify international data transfer.

Firstly, coherent and detailed substantive rules should be created, maybe at EU level, and then procedural rules should be implemented at national level with EU leadership to reach unified interpretation and enforcement. Finally, authorizing procedures may last as long as a whole year with a great deal of work and costs, in strong cooperation with (other) national DPAs as well, which may discourage companies from submitting applications.

5.3.3 Opportunities

Over a longer period of time, applying BCRs as a part of the company's business strategy can be profitable. Having BCRs in place may help win customers and it may reduce or dispense with the need for regular authorizing and/or contracting. It can help avoid suits being brought because of privacy infringement or misuse of

[66] Such as Bulgaria, the Slovak Republic and certain states of Germany.

personal data in case of full obedience. Within the EU, having the GDPR in effect and using BCRs, companies can create a fully compliant data-protection surrounding by the unique and separated self-regulation system. However, this kind of self-regulation may facilitate compliance in fields which have major and systematic problems in data protection, like claims management and debt-collector companies.[67]

An opportunity due to authorizing BCRs is that the companies may evolve better relation to the national DPA as during the authorizing process the company and the DPA should closely collaborate. Applying BCRs a company may even achieve better PR in market competition because having a reliable privacy policy can strengthen good reputation and helps win the trust of customers.

One of the most attractive factors of BCRs may be that the spread of the above-detailed mutual recognition system will encourage companies to apply BCRs, as the authorization process will be shorter, easier and less time-consuming on the way to enjoying the advantages of BCRs in a number of countries.

5.3.4 Threats

How can a code of conduct have binding force? If we deem BCRs as a unilateral declaration then how should we treat the affiliates which are different legal entities established under another jurisdiction of a different country? If we deem BCRs as general terms and conditions then they should have an underlying contract for general or particular data transfer. In case there is no such contract, then this construction can hardly be accepted. If we deem it as a code of conduct it is the company's business decision whether to obey or not.

As for the binding nature of BCRs, the question of jurisdiction can also raise heated debates. What happens if the data subject, the data controller and the data processor are under three different jurisdictions? Which connecting principle should be applied? Which legal regime will be applied to their case? Which national organ or authority can carry out an investigation and who can decide the legal debated? Will only courts have the competence to deal with such cases, including BCR infringements, or will national DPAs also be competent? Can the data subject refer to the BCRs in a suit or during an administrative process or can only statutes state his rights? These questions await an answer from the future.

There have been very few cases in domestic and international legal practice to learn how to deal with these processes. The question arises how DPAs can fight against forum shopping for easier procedures, lower duties and fees or their sphere of discretion.

[67] The Hungarian national DPA in its annual control plans in 2013 and in 2014 put the focus on claim management and debt collector companies because of the high rate of complaints on their activity, available at: http://www.naih.hu/files/NAIH-ellenorzesi-terv-2013.pdf; https://www.naih.hu/files/NAIH_ell_terv_2014.pdf.

Although the burden of liability is laid upon the data controller in the EEA, the sub-processor is not subject to the BCRs nor under the obligations stated therein. Thus, from the point of view of the sub-processor, an adequate level of protection of personal data is not ensured anymore, so the BCRs would miss their final goal.

6 In Conclusion: Bottom Lines

As Laudon emphasizes, digital development cannot be blamed for privacy infringements but we the people of the digital era have created our situation by carelessly providing personal data without limit. In the opinion of the author of this paper the information market has already existed before, but not in such an institutional form, as Laudon stated, and with a difference that the data subject does not have the power to ask for profit from the usage of their personal data.

If we consider privacy as the right to provide personal data which has commercial and strategic value, then it plays a vital role in economic processes, as businesses in the digital economy can use personal data as a major input. Multinational companies in their everyday business have to comply with the rules of international data transfer at national and at EU level as well, which requires time-consuming and expensive efforts. Co- or self-regulation may help these companies to establish a binding framework to ensure an adequate level of protection in third countries while being able to comply with the rules, as these rules are tailored to their specific needs. Personal data obviously embodies high value in a practical sense, as the GDPR in Article 83. enacted differentiated systems of sanctions, which include in respect of the types of the infringements the maximum administrative fines up to EUR 20,000,000, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher in case of data transfer to third countries.

A new solution to this issue and to creating a GDPR-compliant data-protection policy is the application of binding corporate rules. The BCRs themselves can be deemed as a unilateral commitment or a code of conduct which, with its binding rules, can create a legal basis for ensuring adequate safeguards in third countries. The approval procedure may frighten companies, but an authorized set of BCRs is an ultimate guarantee for grounding lawful data-processing mechanisms. Nevertheless, the real impact and suitability of BCRs will become clear only after years of application, as many questions and factors for debate have been raised so far. Although the GDPR does not regulate BCRs for data processors, tendencies show increased interests in this sector as well. Furthermore, a comparative analysis[68]

[68] Article 29 Data Protection Working Party: Joint work between experts from the Article 29 Working Party and from APEC Economies, on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents, Adopted on 27 February 2014, WP212, 538/14/EN.

has also been made on the common points and additional features of BCRs and the Cross Border Privacy Rules submitted to the APEC. Thus, BCRs are not an unprecedented legal concept from a world-wide perspective.

As is highlighted in the SWOT chart, data-protection mechanisms are advantageous factors of businesses. In the chart an equal number of strengths and weaknesses are listed but many other factors can be added. In spite of this until the domestic or the international legal practice has determined clear situations we cannot make confident statements on the application of BCRs. In any case, if a company is committed to data protection—even to the point of applying BCRs—then it should be supported and acknowledged for its commitment.

References

Acquisti, A. (2010), The Economics of Personal Data and the Economics of Privacy, Background Paper #3, OECD, OECD Conference Centre 1 Dec. 2010, available at: https://www.oecd.org/sti/ieconomy/46968784.pdf

Acquisti, A. (2013), The Economics of Privacy: Theoretical and Empirical Aspects, Carnegie Mellon University, first page, available at: https://pdfs.semanticscholar.org/4807/d80005a2dfc8af1d149ddb77096bcc26e488.pdf.

Baker, R.K. (2006), Offshore IT Outsourcing and the 8th Data Production Principle - Legal and Regulatory Requirements - with Reference to Financial Services, 14 International Journal of Law and Information Technology Issue 1, 1 March 2006, pp 1–27.

Csegődi, T. L. (1979), A jog pozitivitása mint a modern társadalom feltétele, In: Jog és szociológia., Válogatott tanulmányok KJK, pp. 123-142.

Finn, R.L. / Wright, D. / Friedewald, M. (2013), Seven Types of Privacy, in: S. Gutwirth et al. / R. Leenes / P. de Hert / Y. Poullet (Eds.), European Data Protection: Coming of Age, Springer, pp 3-32.

Horváth-Egri Katalin (2015), A kötelező szervezeti szabályok (Binding Corporate Rules, BCR) és az együttműködési eljárási lehetőségei, Infokommunikáció és Jog, Vol XII, No 64, HVG Orac Lap- és Könyvkiadó Kft, Budapest, 2015. pp. 143 – 147.

Huang, P.H. (1998), The Law and Economics of Consumer Privacy Versus Data Mining, University of Pennsylvania, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=94041

Kuner, C. (2015), Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law, University of Cambridge Faculty of Law Research Paper No. 49/2015, 2015, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2644237

Laudon, K.C. (1996), Markets and Privacy, Association for Computing Machinery, Communications of the ACM, Sep 1996, Vol 39, No 9, 92-104, ABI/INFORM Global

Luhmann, N. (1979), The unity of the legal system, in: G. Teubner (Ed.), Autopoietic Law: A new approach to law and society, Gruyter

Moorhead P.: Why Your Personal Data Is The New Oil (2011), please give a sourceOros / Szurday (2003), Európai Füzetek 35.: Adatvédelem az Európai Unióban – Szakmai összefoglaló a magyar csatlakozási tárgyalások lezárt fejezetiből, A Miniszterelnöki Hivatal Kormányzati Stratégiai Elemző Központ és a Külügyminisztérium közös kiadványa.

Oros P. / Szurday K. (2003), Adatvédelem az Európai Unióban – Szakmai összefoglaló a magyar csatlakozási tárgyalások lezárt fejezeteiből, A Miniszterelnöki Hivatal Kormányzati Stratégiai Elemző Központ és a Külügyminisztérium közös kiadványa, Európai Füzetek 35., Budapest, 2003.

Posner, R.A. (1978), The Right of Privacy, 12 Georgia Law Review first page.

Posner, R.A. (2011), Economic Analysis of Law, Aspen Publisher

Tóth, J.Z. (2004), Richard Posner és a gazdasági jogelmélet, Jogelméleti Szemle, 2004/1.szám, available at: http://jesz.ajk.elte.hu/toth17.html

Ryngaert, C. (2015) Symposium issue on extraterritoriality and EU data protection, International Data Privacy Law, Volume 5, Issue 4, 1 November 2015, Pages 221–225, Oxford University Press, https://academic.oup.com/idpl/article/5/4/221/2404465

Samuelson, P. (2000), Privacy As Intellectual Property?, Stanford Law Review, Vol. 52, No. 5, Symposium: Cyberspace and Privacy: A New Legal Paradigm? (May, 2000), pp. 1125-1173 available at: http://people.ischool.berkeley.edu/~pam/papers/privasip_draft.pdf

Szabó, M.D. (2005), Kísérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival, Információs társadalom, 44-54.

Szőke, G.L. (2015), Az európai adatvédelmi jog megújítása – Tendenciák és lehetőségek az önszabályozás területén, HVG-ORAC Lap- és Könyvkiadó Kft

Varian, H.R. (1996), Economic aspects of Personal Privacy, In: Lehr W., Pupillo L. (eds) Internet Policy and Economics. Springer, Boston, MA, available at: http://people.ischool.berkeley.edu/~hal/Papers/privacy/

Warren, S.D. / Brandeis, L.D. (1890), The Right to Privacy, Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220.

Wright, D. / de Hert, P. (2016), Enforcing Privacy: Regulatory, Legal and Technological Approaches Law, Governance and Technology Series, Volume 25, Springer International Publishing

Additional Sources

Article 29 Data Protection Working Party: (2003) Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp74_en.pdf

Article 29 Data Protection Working Party: Joint work between experts from the Article 29 Working Party and from APEC Economies, on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents, Adopted on 27 February 2014, WP212, 538/14/EN

Article 29 Data Protection Working Party: WP 74, WP 108, WP 133, WP 153, WP 154, WP 155, WP 176, WP 195, WP 204

European Commission (2015), Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses, Press Release Database, available at: http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en

European Commission (2011), Social Eurobarometer 359 Attitudes on Data Protection and Electronic Identity in the European Union, available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

European Commission (2016), Digital Privacy, available at: https://ec.europa.eu/digital-single-market/online-privacy

The Power Paradigm in Private Law

Towards a Holistic Regulation of Personal Data

Heiko Richter

Contents

1 Introduction 528
1.1 Relevance 528
1.2 The Lack and Need of a Holistic Approach 529
1.3 The Private Power Approach in Private Law 530
1.4 Structure of the Study 532
2 Framing Power in Private Law 532
2.1 Need to Frame Power 532
2.2 Power Concepts 533
2.3 Particular Legal Areas 535
3 Power and Personal Data in Areas of Private Law 535
3.1 Contract Law 535
3.2 Consumer Protection Law 540
3.3 Competition Law 544
3.4 (Intellectual) Property Law 552
3.5 Data Protection Law 555
3.6 Anti-Discrimination Law 560
3.7 Going Beyond: Power of Opinion as a Subject of Media Regulation 563
4 Findings and Implications 564
4.1 Towards a Holistic Approach 564
4.2 Descriptive Findings and Implications 565
4.3 Normative Implications 569
5 Summary 571
References 573

Abstract Currently there is no holistic concept linking the various areas of private law that are concerned with the regulation of personal data. However, there is a strong need for one. This study elaborates on such an approach by focusing on the

Heiko Richter is Junior Research Fellow and Doctoral Student at the Max Planck Institute for Innovation and Competition.

H. Richter (✉)
Max Planck Institute for Innovation and Competition, Munich, Germany
e-mail: heiko.richter@ip.mpg.de

M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law*, MPI Studies on Intellectual Property and Competition Law 28, https://doi.org/10.1007/978-3-662-57646-5_19

private power paradigm. Private power is of utmost relevance for personal data and pervades various areas of private law. This study applies recent findings of research conducted by private law scholars, who have conceptualized private power in private law, to the regulation of personal data in private law, namely in the areas of the law of contract, consumer protection, competition, (intellectual) property, data protection and anti-discrimination. It draws descriptive as well as normative conclusions which can help to better understand the regulatory implications and serve as a methodology for identifying and shaping coherent and prudent regulation of personal data in the future.

1 Introduction

1.1 Relevance

Over the last decade, technological and economic changes have led to new and significant conflicts of interest regarding **personal data**.[1] The accumulation of various developments, such as increased computing power, advanced data mining techniques, an increased amount of available open data and the transfer of previously non-personal data to the realm personal data,[2] has allowed personal data to be processed on a massive scale causing a significant fall in transaction costs in the wake of digitalization. The form in which personal data is being used has shifted from a deliberate to an incidental collection of personal data. Also, a shift from single use to multiple re-uses for varying purposes and the long-term retention of personal data can be observed.[3] These changes drastically affect everyday life.

What are the **consequences for private law**? This study focuses on the question of how private law can deal with the effects of the stated technical and economic developments. In particular, it seeks to elaborate how certain areas of private law can regulate personal data on a holistic basis. It will be seen that there is both a lack of and a need for a holistic approach to the regulation of personal data in private law (under Sect. 1.2). As this study identifies private power as the lowest common denominator for various areas of private law, especially when regulating personal data (under Sect. 1.3), private power will be the guiding paradigm for moving private law closer towards a holistic regulation of personal data.

[1] Here defined according to Art. 4(1) GDPR: "any information relating to an identified or identifiable natural person".

[2] Van Loenen / Kulk / Ploeger (2016), 16; see for distinguishing personal from non-personal data the case AG Campos Sánchez-Bordona, CJEU, Breyer v. Federal Republic of Germany, C-582/14, ECLI:EU:C:2016:339, para. 52 et seq.

[3] Mayer-Schönberger / Padova (2016), 334.

1.2 The Lack and Need of a Holistic Approach

Especially in regard to competition, consumer protection and intellectual property law, practice has shown that there is an increased need for a more **"holistic" approach** when regulating personal data. But what is to be understood as a holistic approach and why is it beneficial? A holistic legal approach must align different legal areas to a particular decision paradigm on the meta-level.[4] As different areas of law follow their own rationales and are based on subject-specific assumptions, an approach must either accommodate such sub-paradigms or justify a change of paradigm within the particular areas if it is to be truly holistic by definition. This necessarily requires an analysis on different levels of abstraction whilst revealing the respective (often implicit) assumptions and discussing them in a systematic and explicit way. While holistic approaches have both explanatory and analytical power on a theoretical level, they can guide regulation to be both effective and legally coherent on a practical level.

In the context of personal data, extensive theories that go beyond the mere discussion and analysis of particular **interfaces** between legal areas cannot be found in the field of private law.[5] So far, legal practice and academia have increasingly observed the status quo and subsequently discussed interfaces and interplays between different legal regimes. As technology, legislation and jurisprudence advance quickly,[6] the opportunity to reconsider the current developments should be taken. At the moment, sufficient policy change and a considerable amount of private

[4] The most prominent—yet deliberately not chosen—paradigm in the field of private law is efficiency. There is a flourishing body of literature on the economics of privacy (see for the starting point Posner (1981) and a most recent elaboration on the streams of theoretical and empirical research on the economics of privacy Acquisti / Taylor / Wagman (2016); in particular on personal data markets (see for a good overview Spieckermann / Acquisti / Böhme / Hui (2015)).

[5] Explicitly calling for holistic approach see European Data Protection Supervisor (2014a); based on that also calling for a more holistic approach to tackle the (personal) data issues, Monopolkommission (2015); first advanced academic step towards a holistic approach (and also going on a more abstract, though not holistic level, referring to court decisions, but still legalistic, in a sense that trying to connect on the horizontal level) Ferretti (2014), in particular Ch. 5: Competition, the Consumer Interest and Data Protection; for a holistic deconstruction of data protection, v. Lewinski (2014), but also taking a conventional public law approach, by identifying actors and objects of protection, not going a step further and proceeding to the power question and only briefly discussed as "limitations of data power", 56; for an ambitious holistic, interdisciplinary project see "EUDECO – Modelling the European Data Economy", but this goes far beyond personal data and has a more industry-focused/economic approach, see EUDECO D1.1 Detailed research framework, Public Report – Version 1.0 – of 17 April 2015.

[6] E.g. technical phenomena related to "big data", multi-layer regulation in the Member States, the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – GDPR) on the EU level as well as various court decisions, e.g. CJEU, Google Spain SL, Google Inc. v Agencia Espanola de Protectión de Datos, Mario Costeja Gonzàles, C-131/12, ECLI:EU:C:2014:217; CJEU, Maximilian Schrems v Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650.

law literature on the subject are available. This could enable a holistic approach on a more abstract level in private law, drawing upon theory and recent evidence.

Holistic approaches, which conceptualize personal data in a more general, non-private-law-related way, have usually been embedded in a broader discussion about **conceptions of privacy**. Such general approaches, also focusing on implications for regulation, predominantly come from American scholars.[7] Even though in Europe, and—for historic reasons—especially in Germany, privacy is traditionally a sensitive and heavily debated topic in different fields as well,[8] there is a traditional divide between public and private law. This is still reflected in the stereotypic approaches taken by the respective academics: Public law scholars prefer to work on general concepts of personal data, privacy and constitutional limitations or constructions of privacy in order to derive certain implications from them (top-down approach). In contrast, private law scholars are rather concerned with the application of a certain legal system and whether legislation is necessary, according to the interests of the parties and the coherency of the legal system (bottom-up approach). The reasoning of the respective discipline, however, mostly stays within its own system and does not connect the discourses on a higher level.[9]

1.3 The Private Power Approach in Private Law

This study aims to fill this gap by developing a holistic approach for the regulation of personal data in those areas of law which have proven relevant for the relations between private actors.[10] The guiding thought is that a holistic approach—by defini-

[7] Amongst many seminal works, those ones which specifically refer to (private) power imbalances: Solove (2001), who pleads for reframing the perception of privacy in the digital age; on the pluralistic conception of the broader phenomenon of privacy Solove (2007); calling for a structural approach to privacy regulation Cohen (2013), also Cohen (2012); Richards / King (2014), for setting out general principles for big data.

[8] For one of the influential, recent works see Rössler (2001); for more polemic approaches, based rather on opinion than on evidence, on the one hand Sofsky (2007); on the other hand Heller (2011), which can be seen as representative for the extreme opinions at the respective ends of the political spectrum.

[9] Sketching the legal framework, but without drawing links (beyond what can be drawn from the constitution): Roßnagel / Richter / Nebel (2012); drawing on single aspects, which might be improved, Masing (2012), but already recognizing the gaining significance of data protection between private actors; focusing on the status quo and interfaces Spindler (2014); as a prototype for a public/constitutional law approach to elaborate on personal data between private actors see Bäcker (2012), which starts with the state-citizen perspective and then discusses duties to protect citizen against citizen, referring to outer limits, as pre-determined by the constitution; seminal in this respect Hoffmann-Riem (1998).

[10] This is an extended understanding of private law, as it also accommodates data protection rules, which regulate the relation between private actors. At the same time, it does not deal with questions of public power, which is a much more explicit paradigm in public law (e.g. theory of subordination), however in a rather formalistic way.

tion—must go far beyond the individual disciplines and their horizontal interfaces on the surface. Rather, it should advance vertically to the common root of the problem of personal data and private law: **private power**. It is based on the—almost trivial—observation that private power is *the* leitmotif inherent to personal data. Framing personal data as a source of private power becomes obvious when referring to Francis Bacon's famous quote "knowledge is power" in conjunction with Max Weber's frequently cited definition of power being "the probability that one actor within a social relationship will be in a position to carry out his own will despite resistance, regardless of the basis on which this probability rests."[11] From this perspective, the much-touted concept of informational self-determination can be intuitively understood as an information-specific principle of autonomy that empowers the individual. Collection and processing of personal data can therefore shift the power balance between private actors.[12] Causes and effects of such shifts have gained a lot of attention in recent years due to the stated technical progress, which has enabled an exponential growth in the collection, storage, processing and dissemination of personal data. The World Economic Forum recognized the importance of power for personal data when it concluded: "These power dynamics serve to frame the narrative for many of the digital dilemmas shaping the personal data ecosystem."[13] Moreover, the European Data Protection Supervisor has referred to an ongoing convergence of "monopoly power and informational power."[14]

This study focuses on private power, as it discusses non-public forms of power. Intuitively, private relations are mainly regulated by **private law**. Also, there is no legal definition for power. As a consequence, one has to ask first how power is reflected and dealt with in private law. One of the major challenges is that there is not a single, universally valid definition of power. Weber's well-known definition of power is one of many, and power is a ubiquitous phenomenon that needs to be defined in a much clearer way in order to be transformed into a workable term for the law. Various concepts of power have evolved over time. Those different concepts are reflected in private law. But drawing a taxonomy is a complex task. A group of German civil law scholars has explored this question.[15] Based on their results, this study develops a theoretic framework and applies it to the regulation of personal data.

[11] Weber (1972), as translated by Warren (1992), 19.

[12] Müller / Flender / Peters (2012), 144.

[13] World Economic Forum (2014).

[14] European Data Protection Supervisor (2016), 8.

[15] Möslein (2016).

1.4 Structure of the Study

Initially, this study will outline a general framework of power and private law concentrating on the need for a concept of private power and describing a power taxonomy (Sect. 2). It will then apply this framework to the regulation of personal data through private law (Sect. 3). For that purpose, this study distinguishes between six **selected areas of private law** which appear most relevant for the regulation of personal data: the law of contract, consumer protection, competition, (intellectual) property, data protection[16] and anti-discrimination. Moreover, media regulation as public law can illustrate where private law finds its limits. Finally, the study will then analyze the findings and discuss their implications (Sect. 4), while strictly distinguishing between descriptive findings and normative implications.

2 Framing Power in Private Law

2.1 Need to Frame Power

Private power is neither a legal nor an otherwise clearly defined concept.[17] It is a ubiquitous phenomenon more or less explicitly defined in various areas of private law. Private law can be described as the regulation of private actors' relationships. Furthermore, it can be seen as a reaction to changes of the perception and the interpretation of social reality and the underlying balances of private power.[18] Therefore, it is not surprising that concepts of power in private law have correspondingly developed into concepts of power in other disciplines.[19] Obviously, at this stage, the connection between private law and power still appears diffuse.

In order to allow legal scholars to deal with "private power" adequately, the term must be **framed** correctly. To achieve this goal, this analysis can draw upon substantial groundwork on this matter: In their seminal interdisciplinary project called "Private Macht", a group of German private-law scholars systematically observed different concepts of power that pervade the respective areas of private law.[20] Out of a vast array of sociological and philosophical definitions of power, the authors identified four different concepts of power as being significantly relevant for private law

[16] Admittedly, data protection law is traditionally understood as public law in Germany. However, it heavily regulates the processing of personal data between private subjects and is based on consent. This conception moves it close to a contractual and private law understanding.

[17] Böhm (1960), 44.

[18] Renner (2016), 511, 519.

[19] Ibid., 507.

[20] Möslein (2016); for discussing private power in private law see also Hauer et al. (2013) and specifically about informational self-determination Buchner (2006).

and arranged them within a taxonomy.[21] This taxonomy was derived from and applied to different areas of private law (such as the law of contract, corporate, property, competition or family), since each concept of power depends on its particular regulatory context.

While the mentioned project does not discuss personal data or private power in particular, the following approach does both. As will be shown, this study proves the validity of the **power taxonomy** by applying it in new areas of law and reveals new insights into the subject matter of personal data as well as the general theory. This taxonomy, which forms the basis for this study, will be briefly outlined in the following.[22]

2.2 Power Concepts

2.2.1 Causal Forms of Power

Max Weber described power as "the probability that one actor within a social relationship will be in a position to carry out his own will despite resistance, regardless of the basis on which this probability rests."[23] This definition of power can be understood as **causal-relational**, because power is seen as a particular cause leading to certain effects.[24] This causality focuses on social relationships, specifically the relations between human actors in society. Being in a position of power allows one actor to unilaterally enforce his interests against the interests of another actor. Typically, the use of power by one actor is detrimental to another actor.[25] In consequence, power can be accumulated, allocated and transferred.

As the factual accumulation of private power progresses, not only are social relations shaped, but private power also causes structures to arise, change or disappear.[26] Such forms of power can be classified as **causal-structural**. Early on scholars realized that a mere relational perception and regulation of power is not sufficient. This need especially became apparent when looking to understand economic power.[27] It is the core observation about power by Walter Eucken and Franz Böhm, the fathers of Ordoliberalism, that economic power reaches beyond single relationships and can shape structures as such and thereby radically affect society.[28] The market economy,

[21] For an overview see Renner (2016), 505-528.

[22] Even though the taxonomy is debatable, the main goal of the study is the application to personal data and not the questioning of the taxonomy as such. However, in the wake of application, some insights can already be gained, which also bear some implications for a further refinement and development the taxonomy.

[23] Weber (1972), as translated by Warren (1992), 19.

[24] Renner (2016), 513.

[25] Rölli (2016), 88.

[26] Eucken (1965), 202.

[27] Renner (2016), 513.

[28] Ibid., 515.

in particular, has fostered a systematic exploration of how private power influences structures. Indeed, the market as an allocation system can be seen as a key structure subject to private actors' power. However, structural power is to be understood quite broadly in this study. It can also refer to structures such as public opinion or society at large. As long as the execution of power is directly linked to the impact on the respective structure, the concept of power is of a causal-structural nature.

2.2.2 Modal Forms of Power

In more modern power concepts, it has been discussed that power must not necessarily be understood as a causal force. Power has rather been framed in a significantly broader sense. It was Niklas Luhmann who developed a **modal-relational** power concept. He focused on the conditions under which social interaction—and communication in particular—takes place. Rather than causes, which lead to certain effects (e.g. force), the circumstances (modalities) of the situation determine the conditions—to be more precise: the scopes of action for the respective actors.[29] Therefore, it is essential to focus on the context of actions in order to understand power, not on the action as such.[30] Even if a particular choice itself is voluntary, the lack of other alternatives in the particular context can indicate modal power.[31] This type of power can have both negative and constitutive functions.[32] As Luhmann has consistently based his model on the assumption of social interaction as a form of communication,[33] his concept of power remains relational.[34]

Michel Foucault went a step further, detaching modal power from social relations and focusing on the structural factors which shape the actors. He saw a reciprocal relationship between thinking and action, which in turn is influenced by given power structures. At the same time, the current way of thinking is mirrored in the structures.[35] Foucault's **modal-structural** perception of power is the broadest and most abstract, as it refers to the power of institutions or social convention as such, which may be hidden behind the daily norms of society.[36] Since he viewed power as a ubiquitous, eternal phenomenon,[37] as a result in his theory there is no type of knowledge that is completely free of power relations.[38]

---

[29] Renner (2016), 516; Rölli (2016), 88.

[30] Rölli (2016), 89.

[31] Renner (2016), 516; Luhmann (2012), 20: "power as a chance to increase the probability of unlikely correlations of selections" ("Selektionszusammenhänge").

[32] Rölli (2016), 89.

[33] Luhmann (2012), 20.

[34] Rölli (2016), 89.

[35] Renner (2016), 517.

[36] Foucault (1976), 122.

[37] Foucault (2015), 239.

[38] Han (2005), 54.

2.3 Particular Legal Areas

Lawyers conventionally subcategorize, think and develop their scholarship within particular **areas of law**. As Kainer and Schweitzer state, the positive law entails numerous places of different implementations and different kinds of power control. It is the task of legal scholarship to systemize these factors in order to develop new norms.[39] While holistic approaches, by their very definition, must observe the links between these functional categories, the areas of law still set the primary order of the following analysis. Thus, the law's default order is connected to the previously stated concepts of power, which tend to be of sociological and/or philosophical nature. This type of approach is unfamiliar to legal scholars, yet power concepts are always implicitly or explicitly reflected in the areas of their observation. Hence this approach could enable a more abstract ascertainment of implications, which in turn is necessary for developing a holistic model of private law with particular regard to personal data.

The **areas** of private law examined here were selected according to their relevance for personal data. As will be seen in the following, the relevance is particularly high for the law of contract (Sect. 3.1), consumer protection (Sect. 3.2), competition (Sect. 3.3), (intellectual) property (Sect. 3.4), data protection (Sect. 3.5) and anti-discrimination (Sect. 3.6). Finally, by looking briefly into the area of media regulation (Sect. 3.7), the implications of public law approaches and their relation to power will be examined. As will be seen, all these areas in turn relate to specific power concepts and they apply to personal data at least to some extent. Ultimately, the concrete application to personal data also challenges the perception of power within the respective legal area as such.

3 Power and Personal Data in Areas of Private Law

3.1 Contract Law

3.1.1 Subject Matter and Regulation of Power

At its very core, contract law reflects implicit and explicit assumptions about power. Therefore, it serves as a starting point for the analysis. A contract is the standard form of regulating the relation between private actors.[40] It is based on **agreement**. Therefore, the presumption of free will and protection of private autonomy lies at the center of contract law.[41] The crucial power-related question is, when does a more

[39] Kainer / Schweitzer (2016), 631.

[40] Berger (2016), 55.

[41] Ackermann / Franck (2014), 169: Provisions of invalidity refer to judicial acts in general and not specifically to contracts, as the presumption and protection of private autonomy is at the center-stage of the German Civil Code (Bürgerliches Gesetzbuch – BGB).

powerful position of one party turn into an illegitimate limitation of the other party's freedom.[42]

Accordingly, contract law already protects the formation and the execution of free will *before* the contract has in fact been concluded.[43] The parties must have the capacity to contract and are protected from binding themselves on the grounds of mental reservation, mistake, fraud, coercion, or threats.[44] In principle, contract law is not concerned with the inequality of the value of exchanged performances. However, contract law invalidates excessive benefits or unfair advantages should one party exploit a procedural defect in the bargaining process to the detriment of the other party (such as dependency, economic distress, urgent need, improvidence, ignorance, inexperience, lack of bargaining skills).[45] The line is to be drawn where the contract is just a "disguise" for unilateral enforcement of will.[46] In this pure form, contract law perfectly reflects the Weberian **causal-relational power** concept[47]: As the main principle of contract, mutual consent legitimizes the power relation in the social relation. Mandatory regulation is linked to causalities that lead to a power imbalance in the relationship between the parties and to an exploitation in the very specific case.[48]

However, contract law also provides a judicial control of terms that are not individually negotiated (standard terms). Its introduction into statutory law arrived rather late.[49] In the case that such terms are contrary to the regimes of good faith or fair dealing, mandatory contract law declares them voidable or void. Judicial control of standard terms targets clauses that have not been negotiated between the parties. It requires neither an actual monopoly of the user[50] nor an information deficit of the contracting partner.[51] Therefore no actual defect leading to an unfair outcome is necessary. Thus, this type of contract regulation is triggered by mere modalities within the social relation of the conclusion of the contract. Hence, it follows a concept **of modal-relational power**. Rather than relying on actual, causal

[42] Herresthal (2016), 160.

[43] Renner (2016), 519.

[44] E.g. §§ 116-124 BGB.

[45] Ackermann / Franck (2014), 211 et seq., who understand § 138 BGB as an expression of "*boni mores*" and "undue influence".

[46] Böhm (1960), 31.

[47] Renner (2016), 519, as opposed to Herresthal (2016), 163 et seq., who has a narrower understanding.

[48] Herresthal (2016), 177 et seq.; Böhm (1960), 32. But see also on legal presumption regarding § 138(1) BGB: BGH NJW 1995, 1019, 1022.

[49] Ackermann / Franck (2014), 233: In 1977, the Act on General Conditions of Business (AGBG) entered into force and turned common case law into statutory law.

[50] Earlier, § 138 BGB was used as a standard to scrutinize standard terms if one party had a dominant position.

[51] Renner (2016), 519.

proof, it is based on the implicit assumptions of information superiority[52] and an exercise of unilateral power.[53] The user of standard terms limits the scope of selection for the other party in advance, which nicely echoes Luhmann's power concept.[54] While the general clause for judicial control of standard terms allows for consideration of the specific facts of the case and also take causal factors into account, at least black clauses refer to mere modalities.[55] As they set the standard of judicial review of consumer contracts, one can see why consumer law takes an even stricter modal-power approach than normal contract law.[56]

As opposed to single-transaction spot contracts, **long-term contracts** can create permanent power relations, due to the longer period of performance exchange they entail. At the time of contract conclusion, future developments are not perfectly foreseeable[57] and therefore incomplete. These contracts can be susceptible to opportunistic behavior and might call for safeguards to counter power imbalances. Contract law provides various safeguards, and they can be especially effective in relationships characterized by high dependencies (and therefore systemic power imbalances), such as employment or lease contracts.[58]

3.1.2 Personal Data

Contracts relating to personal data are also based on consent. Therefore, their validity must be in accordance with the stated general contract law principles. Moreover, **data protection law** requires a higher threshold when it comes to the validity of consent.[59] This is also true for the judicial review of standard terms that relate to the processing of personal data[60] and also include the impermissibility of excessive

[52] Ackermann / Franck (2014), 237 et seq., speaking of information asymmetries, but also of systematic procedural deficiencies in the formation of contracts, due to rational ignorance of a party towards them.

[53] "Take it or leave it", Renner (2016), 510: BGH sees the root of the problem in unilateral power of determination ("einseitiger Gestaltungsmacht"); more critical Herresthal (2016), 133 et seq.

[54] Renner (2016), 520 et seq.

[55] For determining, if that is the case, the German model follows a 3-step approach (see §§ 305 et seq. BGB): First, it contains black clauses (§ 309 BGB), which precisely define such situations without any discretion. Second, grey clauses (§ 308 BGB) are presumed to constitute such a disadvantage, though the single circumstances can be taken into account. Third, a general clause (§ 307 BGB) sets the standard for all clauses, which must not cause a significant imbalance in the parties' rights and obligations arising under the contract.

[56] Canaris (2000), 273 et seq. on the development of stronger material control of standard terms and materialization.

[57] Riesenhuber (2016), 206.

[58] Ibid., 199 et seq., therefore e.g. elaborated construction of termination rights.

[59] E.g. in Germany § 4a BDSG, §§ 12 et seq. TMG.

[60] Bräutigam / Sonnleithner (2015), para. 44; Faust (2016), 36 et seq., considers given rules as largely sufficient.

benefits or unfair advantages.[61] The causal-relational power perception is reflected here, as well as its modal extension. The additional requirements as set out by the General Data Protection Regulation[62] (GDPR) are discussed in the section on data protection, due to their different and more complex power concept.

Without any doubt, personal data can be the subject matter of a contract.[63] However, there is no clear set of rules for contracts under which access to personal data is offered as a **counter-performance** for obtaining other products or services.[64] This has become increasingly[65] relevant in the Internet economy. The provision of digital content—such as in social networks, search engines or map services—is largely offered not for money, but rather for access to personal data. Therefore, the Digital Content Draft Directive[66] explicitly recognizes personal data as consideration for the provision of digital content by setting general rules in case personal data becomes a subject covered by a contract.[67] This regime recognizes the commercial value of personal data that the provider of digital content receives from the data subject. It grants rights to the data subject in case of non-conformity of the content with the contract (Art. 6) and provides for remedies comparable to those granted in cases of monetary consideration.[68] As the Digital Content Draft Directive does not affect data protection law,[69] the obligation additionally requires (unilateral) consent in the data-protection sense.[70] Effectively, only this consent creates extra value, which allows data processing to reach beyond what is already legitimized by data protection laws.[71] Consequently, only this "extra consent" in combination with the obligation can constitute relevant consideration under the Digital Content Draft Directive.[72] But even if consent is given, data protection rules might create tensions: Art. 7(4) GDPR states that if consent was freely given (and therefore valid), account shall be taken of whether the performance of a contract is conditional on consent for the processing of personal data that is not necessary for the performance of the

[61] § 138 BGB is subordinate to AGB-Kontrolle, for the relationship see Armbrüster (2015), para. 5.

[62] See Fn. 6.

[63] BGH Urteil vom 18. Oktober 1989 – VIII ZR 325/88 = ZIP 1990, 1138.

[64] Langhanke / Schmidt-Kessel (2015), 218; even their contractual nature is unclear and disputed, see for a comprehensive discussion Bräutigam / Sonnleithner (2015), para. 38 et seq.; see also Faust (2016), 6 et seq.

[65] Therefore, it has been discussed in contract law, see Schwenke (2013), 37; Dietrich / Ziegelmayer (2013), 104.

[66] European Commission, COM(2015) 634 final, "Proposal for a Directive on certain aspects concerning contracts for the supply of digital content".

[67] Langhanke / Schmidt-Kessel (2015), 218.

[68] See for respective remedies (Art. 12), especially termination rights (Art. 13, 16) and the legal consequences, also Recital 16 Draft Directive.

[69] See Art. 3 No. 8 Draft Directive.

[70] Langhanke / Schmidt-Kessel (2015), 218: Therefore, it introduces contract rules as a parallel layer to data protection rules.

[71] Langhanke / Schmidt-Kessel (2015), 220.

[72] Reflected in Art. 3 No. 4 and Recital 14 Draft Directive.

contract.[73] Obviously this runs against the intent of the Digital Content Draft Directive, which in turn seeks to acknowledge this situation as constituting obligations. Moreover, there are good reasons to argue that the data subject is legally unable to waive the right to withdraw consent.[74] Therefore, the legal consequence of a withdrawal of consent needs to be constructed, as this would affect the performance of the data subject's obligation to provide access to her personal data.

What **power concepts** are affected? First, quite unsurprisingly, the particular rights and obligations between the parties to the contract refer to a causal-relational model. The legal "upgrade" of personal data to the status of counter-performance alters the power balance in that social relation. This power balance, however, ultimately still depends on consent and therefore on causality. Second, there is a modal power strand as well, as the scope of the Digital Content Draft Directive is limited to consumer contracts. Details will be discussed in the next part on consumer protection law. Third, and most interestingly, the Digital Content Draft Directive also explicitly addresses a causal-structural power issue: Rec. 13 states that the Directive seeks to prevent discrimination linked to counter-performances and therefore to business models based on access to personal data. It identifies unjustified incentives for business models to move towards offering digital content in exchange for data.[75] This preventive approach relates to a structural-causal power problem of personal data: By leveling the playing field, the Directive intends to impact the market structure through reducing the incentives that will lead to an excessive amount of digital services being offered for personal data as consideration. Furthermore, to the extent personal data is considered as counter-performance it falls outside the judicial review for standard terms. This is based on the core principle that market forces determine the main subject matter of the contract. The new standard would therefore put more competitive pressure on suppliers of digital content when looking at the scope and conditions of personal data provided as counter-performance.

In terms of the relevant contract law with its reliance on consent-based data protection rules, the nature of the (digital) services provided and the perpetual possibility to process personal data clearly fall under the category of **long-term** performances.[76] The Digital Content Draft Directive provides distinct legal consequences concerning revocation and termination of contracts concerning personal data. The idea is that if there is a defect in performance, the responsible party may not keep the advantages related to the personal data obtained as consideration.

[73] Even more rigid § 28 Abs. 3b BDSG, see also Faust, F. (2016), 7 et seq.

[74] Langhanke / Schmidt-Kessel (2015), 221; this is rooted in Art. 8 of the Charter of Fundamental Rights of the European Union (CFREU); see also Buchner (2006), 272 et seq., for the opposite opinion. A point can be made that there are similarities to intellectual property for that reason; see Hanau (2016), 129, for the discussion of (absolute) paternalism as a reason not to dispose of the object.

[75] Recital 13 Draft Directive.

[76] Especially social media contracts are to be seen as "long-term contracts", Bräutigam / von Sonnleithner (2015), para. 28; see also Faust (2016), 33 et seq.

Therefore, it provides a systematic mechanism for disempowerment of the digital service provider and re-empowerment of the data subject whose personal data is at stake.

3.2 Consumer Protection Law

3.2.1 Subject Matter and Regulation of Power

Since its emergence in the 1970s[77] until this day the search continues for a clear definition and delineation of what consumer law is. Especially in the European legal system, consumer protection does not follow a systematic approach, because regulations are drafted based on a case-by-case policy.[78] This section focuses on consumer *contract* law, as it is private law and presents distinct power implications. The laws on unfair trade practices will not be discussed.[79] The following analysis is based on the assumption that consumer contract law implies a **systematic imbalance between parties** to a contract. The consumer (demanding the good or service for a private purpose) is assumed to be in an inferior position to the trader. This can have different reasons (e.g. economic, informational or psychological-intellectual).[80] Consumer contract law can correct this structural inferiority[81] by adjusting the bargaining environment or regulating the terms of the bargain itself.[82] Therefore, the state curbs the freedom of the parties by setting (semi-)mandatory law[83] that grants special rights and duties to the benefit of the consumer, such as information duties,

[77] On the European level, the Council Resolution of 14 April 1975 on a preliminary program for the EEC for a consumer protection and information policy can be seen as a starting point, OJ 1975 C92/1.

[78] Ibid., 222; Weatherill (2013), 92.

[79] While the respective regimes are highly national, there is an ongoing debate about the core of laws on unfair trade practices and what justifies their existence, see Henning-Bodewig / Spengler (2016). On the EU-level, unfair trade practices are rather treated as consumer protection law (see Köhler (2015), para. 15, about Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market ('Unfair Commercial Practices Directive'), while German law traditionally rather treats it as competition related law (see § 2(1) Nr. 3 AAUC, see also the discussion about § 3a AAUC (formerly § 4 Nr. 11 AAUC)). Accordingly, there must be some market relevant behavior, as the German AAUC protects competitors, consumers and other market participants and interests of the public in undistorted competition, see regarding breaches of data protection laws von Walter (2014). But due to this specific construction, it would be difficult to draw universal power implications and a more carful observation would not significantly add to the debate in this study.

[80] Calliess (2016), 221.

[81] Ibid., 214 about the seminal judgment of the German Federal Constitutional Court on sureties ("Bürgschaftsentscheidung"), see BVerfG, Urteil v. 19.10.1993 – 1 BvR 567/89, 1044/89; for a more economic explanation see Kerber (2016), 643 et seq., elaborating on remedying market failures through information and rationality failures of consumers.

[82] Weatherill (2013), 144.

[83] Calliess (2016), 218.

formal requirements, withdrawal rights or a strict judicial review of standard terms.[84] This is the case for example with doorstep selling and distance contracts, consumer credit agreements or consumer good sales contracts. The consumer is also protected through judicial review for consumer standard terms or special product liability rules.

Consumer contract law is interaction-related, as its application is limited to the relationship between the parties to the contract.[85] In effect, it increases the degree of the consumer's self-determination by preventing or decreasing power imbalances. As opposed to conventional contract law, there are good reasons to argue that consumer contract law follows a modal (and not a causal) power concept: Its application is based on the general assumption of a structural, unequal distribution of power between the parties to a contract, which is presumed to influence the negotiation process to the consumer's disadvantage.[86] Speaking in terms of Luhmann's **modal-relational power concept**, the application of consumer law relies on the assumption that the power imbalance limits the scope of selection of the consumer before the conclusion of the contract.[87] Currently the law treats this imbalance as unchangeable.[88] Due to that deliberate abstraction by the legislature, no actual causality in the particular relationship is needed for the consumer law regime to apply. The law specifies situations in which these imbalances are presumed to occur. Therefore, consumer contract law combines the sociological theory of structural imbalance with a situative model of protection.[89] And even on this more granulated scale, it is the mere modality and not a causality which triggers the application of consumer law.

3.2.2 Personal Data

A **stricter judicial review of standard terms** (such as black lists) usually applies in the consumer-trader relationship. This can also apply to issues related to personal data. However, this is based on the assumption of power imbalances due to the negotiation process and is not a personal-data-specific problem.

As already mentioned above, the **Digital Content Draft Directive** only applies to consumer contracts and therefore is to be categorized as consumer contract law. The Draft Directive puts emphasis on the protection of the consumer's economic interest in the equivalence of exchanged performances. It does not, however, directly intend to protect privacy or personal integrity, even if it might do so in effect. Still, the implicit assumption of a power imbalance is related to personal data. Certainly,

[84] Ibid., 227 et seq. It is, however, difficult to determine a ranking. In regulatory practice, a combination of several measures is common, 233.

[85] Renner (2016), 522.

[86] Calliess (2016), 216; Renner (2016), 521 on producer sovereignty according to Gailbraith.

[87] Renner (2016), 521.

[88] Ibid., 511.

[89] Ibid., 522.

digital content providers supplying digital mass products predominantly affect consumers. The Directive seeks to correct deficits that cause consumers to excessively give away their personal data in order to obtain digital content.[90]

This poses the general question whether **data protection laws** can in fact be considered as consumer protection law or if better protection of consumers could be achieved by further developing data protection laws accordingly. This question can be answered on a formal and on a material level. The formal answer to the question is negative, since data protection laws apply regardless of the fact whether the data subject is a consumer or not.[91] However, on the material side, the interests of a data subject and a consumer overlap to a considerable extent. Data protection meets the (long term) interest of consumers and ultimately also protects them. This might explain why in the United States privacy has been primarily considered a consumer protection issue.[92] And as the Digital Content Draft Directive shows, the commercialization of personal data poses risks mainly to consumers, yet so far data protection legislation has barely been accepted as consumer protection law.[93] For our purpose of developing a holistic approach, however, both answers are unsatisfying as they provoke circular reasoning. One should rather examine on a higher level of abstraction whether the underlying concepts of power, in consumer law on the one hand and in data protection law on the other hand, coincide. This approach will be discussed later when elaborating on the power concepts behind data protection laws. Quite interestingly, German law provides a recent example of declaring data protection rules as consumer law, even though this was done to compensate for an enforcement deficit rather than on material grounds. The German legislature has recently extended the consumer associations' ability to seek and enforce injunctive relief for breaches of data protection law. This extension happened even though individual data subjects had disincentives to pursue litigation, due to high costs and low individual damages, while on the institutional level, only data protection authorities could initiate proceedings, which often came too late due to limited capacities.[94] Up until this amendment, the German Act on Injunctive Relief (UKlaG) did not apply to breaches of data protection laws, because it required a breach of consumer protection laws. However, the German civil courts did not consider most data protection provisions to be consumer protection law.[95] The recent amendment

[90] Calliess (2016), 217.

[91] The word "consumer" is neither used in the GDPR nor in the Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive), which apply to all data subjects (see also German exception for credit contracts in § 29 BDSG).

[92] Harbour / Koslov, (2010) 773.

[93] Langhanke / Schmidt-Kessel (2015), 219, on whether data protection law is to be seen as consumer protection law.

[94] BT-Drs. 18/4631, 11 et seq.

[95] Ibid., 2, on the problem of § 3a AAUC (formerly § 4 No. 11 AAUC): There was considerable debate and many cases before the regional courts, where it had been tried to enforce data protection laws by means of unfair trade laws. There is, however, no ruling by the highest courts.

of the UKlaG now allows consumer and other associations (§ 3 UKlaG) to take action on their own initiative or at the request of consumers, competitors or employers. The newly inserted § 2(2) No. 11 UKlaG explicitly defines data protection rules as "consumer law" within the meaning of the UKlaG. This is the case if they relate to either the collection of consumers' personal data or its processing for broadly defined purposes, namely advertising, market research and public opinion surveys, operation of credit reporting agencies, creation of personality and usage profiles, address and other data trading and other similar commercial purposes. By this means, the legislature hopes that more funds are put into an effective enforcement of data protection, which should benefit the general public and also serve as a warning signal to data protection authorities.

But what are the **power concepts** the discussed cases demonstrate? By its very conception, consumer contract law tackles a form of relational power, as it limits its application to the parties of a contract. Not surprisingly, the strict judicial review of data-related standard terms and contracts on the provision of digital content refer to a relational power concept. While agreement builds the causal core for a transfer of power by a grant of access to personal data within the contractual relationship,[96] the modal rationale of systematic power imbalances also applies due to one party's position as a consumer. The Digital Content Draft Directive defines modalities under which such an imbalance is to be presumed. The imbalance is related to the specific (negligent) situation when the offering of data in exchange for services defines the distinct character of the relevant modality. Furthermore, consumer contract law demonstrates various techniques of correcting power imbalances, of which some measures interfere with private autonomy rather than empowering the data subject by strengthening self-determination.[97] The reform of the UKlaG exemplifies a factual redistribution of power by strengthening effective means of enforcement to the benefit of consumers.[98] Even though this is also regarded by the GDPR as an important means to effectuate data protection rules,[99] one must note that it does not change the substantive standard for legitimate exercise of power, as it simply refers to the breach of data protection rules.

[96] Consent according to § 2(2) S. 2 UKlaG becomes only relevant if it concerns personal data, which go beyond what is allowed for by data protection law. This is in line with the ratio of the Digital Content Draft Directive.

[97] Buchner (2006), 103, remarks that power imbalances related to personal data are not new, but the solution is an effective right of self-determination.

[98] BT-Drs. 18/4631, 2.

[99] Art. 80(2) GDPR explicitly allows for that, see also BT-Drs. 18/4631, 14.

3.3 Competition Law

3.3.1 Subject Matter and Regulation of Power

Competition law regulates the behavior of undertakings in a market context and **protects the process of competition**.[100] Its central provisions concern the ban of cartels (Art. 101 TFEU), the prohibition of abuses of dominant positions (Art. 102 TFEU) and merger control. Modern EU competition policies are mainly driven by the idea that competition rules seek to promote efficiency and maximize consumer welfare.[101] However, there is still considerable debate about the normative foundations as well as the ultimate goal of competition policies[102] and about how to define and conceptualize this goal in detail.[103] Moreover, there is an ongoing debate on whether and to what extent competition rules should take account of other public interest considerations.[104]

Regulating private power lies at the very heart of competition law.[105] All competition law provisions more or less explicitly refer to power. While Art. 102 TFEU requires a "dominant position" and merger control refers to a concentration that would significantly impede effective competition "as a result of the creation or strengthening of a dominant position" (Art. 2(3) European Merger Regulation), Art. 101 TFEU implicitly requires an appreciable restraint of competition and therefore a certain amount of power.[106] EU competition law regulates a **causal-structural form of power**: Competition rules relate to competition in markets as such and therefore to competitive markets as a "structure". The application of these rules does not require an individual relation between particular market actors. Rather, legal intervention targets the kind of power that determines the possibilities to disturb competition and not to harm a particular consumer.[107] Therefore, European competition law reflects the view that its intervention in private autonomy is based not on a party's economic dependency on a market participant, but on the functioning

[100] Schweitzer (2016), 452 et seq.

[101] Wish / Bailey (2011), 3; about consumer welfare European Data Protection Supervisor (2014a), para. 15; Drexl (2011), 314.

[102] See Vanberg (2011), 44 et seq., on consumer welfare, total welfare and economic freedom.

[103] See Ferretti (2014), 93; Zimmer (2011); Hellwig (2006); Basedow (2007).

[104] On Art. 101 TFEU (ex-Art. 81 EC) Roth (2006); Zimmer (2011) on the moral quality of competition law, 76 et seq.; Ferretti (2014), 94, argues, that especially after the Lisbon Treaty, the neoliberal stream and the Commission's policy, which focuses merely on economic interests, has changed by focusing on the social market economy, which enables for considering other public interest considerations and human rights.

[105] Hanau (2016), 131.

[106] Schweitzer (2016), 461.

[107] Ibid., 464; Buchner (2008), 725: Only the effects of certain measures on competition are relevant; Ferretti (2014), 96, argues that competition law concentrates on certain market processes, whereas consumer law focuses on specific transaction between consumer and undertaking, so consumer take different roles in both regimes.

of the market itself.[108] It must be noted that German competition law indeed contains some provisions which deal with a relational form of power in the case of an abuse of relative market power (§ 20 Act Against Restraints of Competition (GWB)).[109] As competition law is based on conduct, such as facilitating cartels or abusing dominance,[110] it requires a causality between the market participant's conduct and the effects on competition.[111]

The European view, that an interaction-related understanding of power is not sufficient for regulating economic power,[112] dates back to Franz Böhm and Walter Eucken, who feared that powerful private actors could determine or at least influence the rules of the market.[113] While market structure reflects power distribution and vice versa,[114] competition was seen as a means to disseminate power, to prevent exploitation and ultimately to preserve the freedom of the market actors.[115] Böhm and Eucken emphasized the fact that this economic power also influences society, so that competition guarantees an equal distribution of power, which is a necessary condition for stable democracies.[116] This formative idea of **Ordoliberalism** points to the negative consequences of private power and has significantly influenced the development of European competition law, though the principles have certainly been considerably modified and refined over time.[117]

As a more general insight, structural concerns of private power have significantly increased in the wake of industrialization and are therefore an inevitable result of modern market economies. Though competition law regulates private power in effect, there seems to be no general legal term of economic power itself that would justify intervention.[118] Rather than being founded on a general theory of power, competition law follows its functional conditions—the protection of competition.[119] However, concentration of private power is a source of harm to competition.

---

[108] Eucken (1965), 202.

[109] Schweitzer (2016), 464 et seq., who is rather critical in this respect.

[110] On the predominant view that dominant position per se is not harmful, as an extension to Eucken's view, see Behrens (2015), 8.

[111] This can also be based on a non-rebuttable presumption, as the regulation of hardcore restrictions under Art. 101 TFEU illustrates, see Schweitzer (2016), 468. However, this does not change the fact, that infringement requires causality, as it refers to concrete conduct and not to mere modalities; see also Körber (2016b), 351 et seq., distinguishing between strict causality and normative causality.

[112] Renner (2016), 513, see also Rölli (2016), 90.

[113] Renner (2016), 514. In fact, already the American creation of the Sherman Act (1890) targeted concentrations of private economic power because of its detrimental effects on the society and democracy at large, see Schweitzer (2016), 452 et seq.

[114] Eucken (1965), 202: manipulation of the equilibrium between supply and demand.

[115] Böhm (1960), 32, 41; Eucken (1965), 201 et seq.

[116] Renner (2016), 515.

[117] Good overview in Behrens (2015), 11: At least from an ordoliberal view, competition is protected as a system within individuals are free to make their choices on the market.

[118] Schweitzer (2016), 471.

[119] Ibid., 472.

Therefore, competition law poses a **prime example** of a legal area which systematically deals with the forms, causes and effects of power in different functional contexts.

3.3.2 Personal Data

Privacy concerns and in particular personal data have become **increasingly relevant** for competition policies.[120] The Google/DoubleClick merger (2007)[121] and the threat of potential global concentration of private power by corporations—such as Google and Facebook—have significantly intensified the debates on both sides of the Atlantic about the interfaces and the interplay between competition, consumer protection and privacy.[122] At the working level, the debate is focused on the challenges of addressing privacy concerns in competition policies and making competition law applicable for this purpose.[123] After initial reluctance, calls for concepts have been voiced. The ongoing gradual shift in current competition policies will be illustrated in the following, as it bears remarkable power implications.

To start with, there is considerable debate on how to **define markets** in the competition context, and specifically on whether market definition should rely on access to personal data and not on competition.[124] Competition authorities and courts are increasingly acknowledging markets for personal data in the "for free" platform

[120] Monopolkommission (2015), Ch. 1, para. 10 and BT-Drs. 18/4721, 3, show that the role of data protection for competition policies has been recognized, though so far, the Commission did not rule in any case that the collection or use of personal data was a violation of competition laws, see Almunia (2012), 4.

[121] In the U.S. F.T.C. Statement of December 2007, File No. 071-0170; in the EU European Commission, Case No. COMP/M.4721, 11 March 2008.

[122] The trigger was the Dissenting Statement of Commissioner Pamela Jones Harbour in the matter of Google/DoubleClick (2007), F.T.C. File No. 071-0170. For the first notable academic approach on the competition and privacy interface see Picker (2008). An early exception in German literature, which recognized knowledge as power, however, very briefly and only from a competition and consumer protection view, not generalizing it for private law as such, Buchner (2008), in reaction to FTC merger decision on Google / DoubleClick. The discussion of data power as market power had then been further elaborated on by Harbour / Koslov (2010). For a rather policy and economics oriented approach on the interfaces see Pasquale (2013). Cooper (2013) connected the debate to the constitutional discourse. Regarding EU-law, the relevant issues were first systematically spotted by Geradin / Kuschewsky (2013) and combined in Kuschewsky / Geradin (2014). Finally, Kerber (2016) discusses the links between the fields from the law & economics perspective takes.

[123] Monopolkommission (2015), Ch. 1, para. 65, according to which current competition law is not sufficiently suitable for solving problems of abuse of a dominant position in case of excessive access to personal data.

[124] See for a comprehensive discussion Bundeskartellamt (2016); also European Data Protection Supervisor (2014a), para. 57; Geradin / Kuschewsky (2013), 14; Monopolkommission (2015), Ch. 1 para. 29 et seq.; Ferretti (2014), 114; Evans (2011), 25 et seq.; Harbour / Koslov (2010), 773, addressing "free" markets for e.g. social networking, mapping, email, photo sharing, calendaring and document management.

economy context.[125] Also, the German legislature has introduced a provision which states that the fact that a service is provided for "free" does not mean that no market exists.[126] In this way, competition law can account for the interests of the data provider, by acknowledging it as a market participant.[127]

At the same time, it has been increasingly recognized that personal data can relate to **market power**. Especially in the Internet economy, market power results from economic and technical features inherent to the respective business models, which have a natural tendency to create market concentration.[128] Significant competitive advantages can be gained and secured by a company that has the ability to collect, analyze and use the data.[129] As a result of this "data advantage", market positions can be difficult for competitors to challenge.[130] Proposals have been made to adjust the competition standard for assessing market power.[131] The German legislature included a provision for two- or multi-sided markets in § 18 GWB to clarify that one needs to take an undertaking's access to information into account when assessing its market position in comparison with its competitors.[132] The provision acknowledges that market power can also rely on (exclusive) access to personal and non-personal data in response to the extensive growth of digital business models and platforms.[133] But this is only one of various factors that should be taken into account when assessing market power and that should by no means be preclusive. In addition, the approval of critical mergers by authorities will depend on improved criteria in order to prevent dominant market positions that rely on uncontestable advantages based on personal data.[134]

---

[125] See European Commission, Case No. COMP/M.7217 – Facebook/WhatsApp, 3 October 2014; Bundeskartellamt, Online-Immobielienplattformen, 25 June 2015, B6-39/15, and Online-Datingplattformen, 22 October 2015, B6-57/15; opposite opinion Franz / Podszun (2015), OLG Düsseldorf, Beschluss v. 9.1.2015 – VI Kart 1/14 (V), para. 43; for a good overview of the recent debate Bundeskartellamt (2016), 36 et seq.

[126] Bundesministerium für Wirtschaft und Energie, Referentenentwurf eines Neunten Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen of 1 July 2016 (RefE 9. GWB-ÄndG), 10: introduction of a new § 18(2a).

[127] Buchner (2008), 726.

[128] Network effects, though the European Commission argues in Microsoft/Skype (European Commission, Case No. COMP/M.6281 – Microsoft/Skype, 7 October 2011, para. 108 et seq.) that the position based on network effects in the particular case is contestable. See also Monopolkommission (2015), Ch. 1 para. 32 et seq. on the general relationship between dynamic markets, portfolio effects, economies of scale, two-sided-markets, lock-in and para. 5 on the business models in the data-driven economy.

[129] RefE 9. GWB-ÄndG, 51; Buchner (2008), 727.

[130] RefE 9. GWB-ÄndG, 51.

[131] European Data Protection Supervisor (2014a), para. 58 et seq.; for conventional methods Monopolkommission (2015), Ch. 1 para. 26 et seq. (referring to the Lerner-Index); Hoofnagle / Whittington (2014); Competition and Markets Authority (2015).

[132] RefE 9. GWB-ÄndG, 10: new § 18(3a) No. 4.

[133] Ibid., 48.

[134] RefE 9. GWB-ÄndG, 73, referring to the Facebook/WhatsApp acquisition.

Furthermore, the question of when the behavior of an undertaking in matters of personal data should be considered an **abuse** of dominance is heavily debated. The discussion addresses several forms of abuse,[135] two of which are particularly striking. First, the interface with data protection laws is currently being refined.[136] As data protection regimes undoubtedly have an effect on competition,[137] the crucial question is whether competition law can actively account for breaches of data protection law and if so, how close the connection should be. Is a mere breach of data protection rules by a dominant undertaking enough or does it have to be particularly related to the competitive process?[138] The German Federal Cartel Office (Bundeskartellamt) has initiated proceedings against Facebook, due to the suspicion that their terms of service may constitute an abuse of a dominant position in the market for social networks.[139] Facebook is alleged to have used terms and conditions on user data that violated data protection provisions due to their intransparency.[140] Second, it is also contested whether personal data can be seen as an essential facility.[141] Assuming that a refusal to supply data fulfills the exceptional circumstances test as set out by case law,[142] granting access to this sort of information can be an appropriate behavioral remedy to eliminate competition concerns.[143]

In a broader sense, one should ask how competition law can **accommodate privacy concerns.** The answer to this question can be approached endogenously and exogenously. On the endogenous side the literature discusses approaches which aim to align the level of data and privacy protection. Competition law should take privacy protection into account by understanding it as relevant for consumer welfare.[144]

---

[135] Körber (2016a), 306 et seq.

[136] But see also CJEU, Allianz Hungária, C-32/11, ECLI:EU:C:2013:160. A breach of laws in other areas can also be a factor to be considered when evaluating infringement of competition law. Therefore, a violation of data protection laws might also indicate an infringement of competition laws, see European Data Protection Supervisor (2014b), 3.

[137] Körber (2016b), 349.

[138] See for a comprehensive evaluation of European and German law and relating to Facebook Franck (2016), 137; Schweitzer / Fetzer / Peitz (2016), 51 et seq.; see also Körber (2016b), 353.

[139] Körber (2016b), 352 et seq.

[140] See Bundeskartellamt, Press Release, 2 March 2016, available at: http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.htm; Ferretti (2014), 110, arguing that as long as data protection standard is not violated, it cannot be an issue of competition law.

[141] Monopolkommission (2015), Ch. 1 para. 34 et seq.; Geradin / Kuschewsky (2013), 13 et seq.; Abrahamson, (2014), 867; critical view Körber (2016a), 308 et seq.; Schweitzer / Fetzer / Peitz (2016), 49.

[142] See recently Drexl et al. (2016), para. 32 et seq.

[143] As the strictest form of market intervention (and in this case a diffusion of structural power), also divestiture is discussed, see Frenz (2014), 194, who argues that the data protection principle of "data separation" shares similarities with "informational divestiture".

[144] See for concepts Swire (2007), 2; Ferretti (2014), 111 et seq., wants consumer aspects to be included under the Art. 101(3) TFEU test and justifies his position with Art. 169 TFEU (competence on consumer protection); Cooper (2013), 1134 et seq., rejects a "privacy-as-quality analogy"; European Data Protection Supervisor (2014a), para. 40, 71, understands data protection as a

Dominant firms might deprive consumers of meaningful privacy choices and therefore lower consumer welfare.[145] As there is usually no price competition, the remaining factors amount to quality.[146] As a consequence, debates on the interface of competition and privacy try to find common ground in this matter. Certainly, it is not without obstacles to define consumer preferences for privacy and to determine a right measure.[147] Also, it can be argued that personal data improve service quality.[148] Therefore, the right measure would be a matter of what to take into account for the sake of consumer welfare and what can be balanced and consolidated. On the exogenous side, the crucial question is whether competition law also protects other policy goals. Moreover, one could use competition law to support other public policy goals, in particular the protection of privacy.[149] Accordingly, it could be argued that the competitive process not only protects the economy, but also the social life of consumers, and that therefore the legal system as a whole—including competition law—should protect fundamental rights more actively.[150]

The most radical approaches move away from requiring abusive conduct and perceive the dominant position of data holders as such as a threat, at least when it is not contestable. **Unbundling** is discussed as the most radical means of disempowerment.[151] In 2014, the European Parliament called for tougher regulation of Internet search systems. The resolution calls on the EC "to prevent any abuse in the marketing of interlinked services by operators of search engines" and "to consider proposals with the aim of unbundling search engines from other commercial services" in the long run.[152] This proposal was not only triggered by the—presumably—not contestable accumulation of power by search engine operators, but also by the fact that it is personal data as such that fuels this dominance.

---

factor of consumer welfare, and proposes privacy-promoting remedies in competition decisions as a consequence.

[145] Dissenting Statement of Commissioner Pamela Jones Harbour in the matter of Google/DoubleClick (2007), F.T.C. File No. 071-0170, 10, footnote 25; Cooper (2013), 1131; European Data Protection Supervisor (2014a), para. 79, referring to Coates (2011), Competition Law and Regulation of Technology Markets.

[146] Evans (2011), 13.

[147] European Data Protection Supervisor (2014a), para. 81; Pozzato (2014), 469; more general about the limitations of the predictability of consumer interests and conflicting interests, Drexl (2011), 318 et seq.

[148] Körber (2016a), 305.

[149] Körber (2016b), 355.

[150] Ferretti (2014), 117; rather opposite opinion Frenz (2014), 195, 200; an analogy can be drawn to the diversity of the media, which lies in the general interest of democratic societies. While this special concern is reflected in special rules for media competition law, one could think about extending that ratio to privacy concerns, see European Data Protection Supervisor (2014b), 3.

[151] See § 41a GWB of the proposal of the Bundesministerium für Wirtschaft und Technologie of 5 May 2010, according to Schweitzer / Fetzer / Peitz (2016), 57, but not in the personal data context.

[152] See The Guardian, available at: https://www.theguardian.com/technology/2014/nov/27/european-parliament-votes-yes-google-breakup-motion.

Without any doubt, the collection or use of personal data can constitute **significant structural power**, especially in the data-driven economy, where business models are systematically based on the processing of personal data. Three factors seem striking: First, the amount of power granted is significant, because platform-based business models have a natural tendency toward concentration. If therefore the competition is not *on* the market, but *for* the market,[153] and the market is defined by the access granted to personal data, it can be concluded that the competition at issue is competition for access to personal data. Second, the fast pace and explosive spread of such business models explains why the law is still at an early stage of looking for answers. Competition law traditionally focuses on the functionality of the price-building mechanism of the market[154] and not on the relation between undertaking and data subject. This poses specific, not yet solved problems, as it raises a fundamental question: What is the "price"-building mechanism for personal data in fact and do conventional economic categories of thought in terms of markets and market failure apply at all? Third, so far even the concepts discussed in competition law still only relate to a structural power concept. Even if competition law considers privacy as an interest of consumers by modifying market definitions, the focus of the inquiry always has to be the structural effect that relates to the power. There is, however, some regulatory action which combines structural with relational elements: the introduction of portability clauses. As this takes place in the data protection regulation, it will be discussed under Sect. 3.5.

Conventionally, particular types of power-related behavior constitute the abuse of power. But because technically every sort of action can have an impact on the market structure and shift power balances, one needs additional criteria to determine when the use of power is illegitimate.[155] Most of the debate around personal data and competition focuses precisely on defining and conceptualizing those criteria. As has been shown, however, there are also some extreme concepts which loosen the causal nexus as they try to condemn the dominant position as such.[156] But if the dominant position—meaning a certain amount of structural power itself—becomes the yardstick for legal intervention, the **power model extends from a causal to a modal concept**. The most radical approach is the breakup of undertakings. The motives for proposing a breakup can differ in the personal data context: The fear that an undertaking has a competitive, personal-data-based advantage which will be uncontestable in the future is mixed with the suspicion that the way such a dominant player can use the data will be to the detriment of privacy.[157] The shift to modal considerations resembles the original narrative by Böhm in the early

[153] Monopolkommission (2015), Ch. 1 para. 22.

[154] Renner (2016), 524.

[155] Ibid., 528.

[156] European Data Protection Supervisor (2014b), 4.

[157] See intensive debate in the Frankfurter Allgemeine Zeitung on Google and Axel Springer, available at: http://www.faz.net/aktuell/feuilleton/debatten/mathias-doepfner-s-open-letter-to-eric-schmidt-12900860.html.

days of Ordoliberalism[158]: His underlying presumption that private dominance as such is to be condemned follows a modal-structural understanding of power. But this resemblance works only at a superficial glance. Interestingly, the freedom that Böhm saw endangered was the "freedom of competition", by which he refers to the freedom of buying and selling for prices, which would ultimately succeed under conditions of perfect competition (as-if consideration). The price was seen as the determinative indicator for scarcity and therefore for an adequate allocation of goods.[159] By no means, however, can personal data be seen as such an indicator for scarcity. Besides the fact that due to their informational nature, personal data are non-rivalrous in consumption, it is their qualitative, rather than their quantitative features, that matter. It is not clear and probably not feasible to determine what the rate of access (meaning how much and what is given in exchange) to personal data under perfect competition would be. This illustrates why, when talking about a shift to modal-structural power theories in the personal data context, we should not speak of a renaissance of a debate (and why it is right to reject this strict approach, as we have learned through the further development of Ordoliberalism), but rather of entirely new terrain.[160]

Another aspect of structural power relates to the function of markets: Markets themselves are understood as instruments for structural **disempowerment**.[161] In this view, market failures cast doubt on the effectiveness of power distribution. Especially the essential facility discussion presents a fundamental power dilemma. On the one hand, stimulating competition by granting access to data diffuses market power through the sharing of personal data. But at the same time, granting access to personal data increases an undertaking's power vis-à-vis the individual the personal data refers to. Speaking in terms of power: While structural power decreases, relational power increases. It is not clear whether competition law should or even can account for this power trade-off.[162] The complex interrelation between structural and relational power illustrated here demonstrates that it would be too short-sighted to compare market mechanisms for price building with market mechanisms involving personal data and to propose the strengthening of consumer sovereignty as a solution.[163] This insight stresses the importance of not confusing monetary payment with data in their different functions when considering them as market parameters: Monetary payment can be substituted and is neutral in particular social

[158] On the train of thought of Franz Böhm, see Hellwig (2006), 241 et seq.

[159] Hellwig (2006), 244.

[160] Also in the regulatory context of the utilities, it was the price, which had been of concern and raised calls for divestiture regardless of abusive practices in the German energy market.

[161] Bäcker (2012), 106, 108.

[162] Without a doubt, protection laws affect the concern of relational power; European Data Protection Supervisor (2014a), para. 67; see also French Competition Authority, GDF, Opinion No. 10-A-13 of 14 June 2010 and EDF, Decision No. 13-D-20 of 17 October 2013; Körber (2016b), 350.

[163] This claims Körber (2016a), 306 et seq., but very generally refusing the data-is-power-analogy as merely political claim.

relations. Personal data, however, is necessarily attached to a personal relation, once access to it is provided.

3.4 (Intellectual) Property Law

3.4.1 Subject Matter and Regulation of Power

Property concerns a legal position of a subject that is directly linked to a thing.[164] In detail, concepts of property significantly differ between jurisdictions.[165] It shall be assumed that property contains the rights to exclusively use, alter, transfer or destroy the thing to which it refers. These rights are of an absolute nature, which means that they have an effect *erga omnes.*[166] In case of infringement, there is a chance to enforce these rights.[167] Property is defined by the law and therefore the legal definition allocates goods. On this basis markets can function and re-allocate the goods.[168] Intellectual property, in particular, refers to creations of an intellect, and therefore to rights in intangible, qualified information. Various approaches seek to justify property rights, defining them for example as a reward for labor, as an expression of personality, as a basis for freedom or in terms of economic utility.[169]

Property is an **allocation of power**, as it entitles an owner to exclude others. Therefore, property law is one of the most prominent examples of regulating private power. Lehmann states that property touches on multiple power concepts: Property has a causal power dimension, as the chance to enforce respective rights can influence another person's will, but also has modal implications, as the (initial) assignment of property limits the choices of others *ex ante*.[170] Moreover, property has a relational power character, since absolute rights apply *erga omnes*, which means that exclusive rights ultimately apply to all individual social relations.[171] Finally, property also has structural elements, because property allocation in sum shapes the very basic conditions of the market and of society.[172]

When inquiring into the relevance of property for personal data, some **specific features** are worth mentioning: As property is a legally constructed form of power,

[164] Cashin Ritaine (2012), 13.

[165] See Cashin Ritaine (2012) for a good overview of the European property regimes. Private property should not be confused with the economic property rights approach, which is broader, see Schäfer / Ott (2005), 549.

[166] Purtova (2011), 80 et seq., comparing common and civil law property regimes and concluding the *erga omnes* effect as their lowest common denominator.

[167] Lehmann (2016), 284 et seq.

[168] Hellwig (2006), 236.

[169] Lehmann (2016), 292 et seq.

[170] Ibid., 289.

[171] Ibid., 284.

[172] Ibid., 289 with reference to the Marxian perception of property.

policy makers always have to consider why and to what extent power should be granted. A property-based position of power is strong, because it is absolute and exclusive. If property rights support already existing factual power, this can further strengthen power.[173] As property can change owners as a consequence of re-allocation, power can also be transferred.[174] At the same time, *private* property also leads to the highest degree of power diffusion from a structural point of view.[175]

3.4.2 Personal Data

For more than three decades it has been debated whether personal data should be treated as (intellectual) property.[176] But despite the ongoing debate and various proposals, there is no jurisdiction that grants property rights in personal data.[177] One must not confuse the question of treating data as property with the **role of data protection laws**. The latter do not initially assign exclusive rights in personal data by default and can therefore not to be said to be property laws.[178] Rather, they assign rights as the outcome of a compromise between individual control and informational self-determination of the data subject on the one hand and the free flow of information on the other hand.[179]

Basically two strands of **motivation** for the introduction of property rights in personal data exist: First, exclusivity strengthens control over one's own data, forcing others to negotiate with the owner and thereby taking multiple interests into account.[180] Second, introducing property to personal data is an adjustment to *de facto* commodification of personal data.[181] Therefore, property in personal data can serve as a tool for enabling market exchange, which can ultimately lead to an

[173] Ibid., 286.

[174] Ibid., 291. Many jurisdictions, such as Germany, legally define and limit the scope and content of property (*numerus clausus*), when it comes for granting rights or transferring rights, see 299 et seq. However, the transfer of personal data seems different, because the intangible good is not rivalrous in consumption. Therefore, limits to property are not as strong as in the tangible world, Buchner (2006), 287.

[175] Lehmann (2016), 296 et seq.

[176] Purtova (2015), 2: An increasing commodification of personal data in the US triggered a debate as to whether or not treating personal data as property already in the early 1970s, while Europe joined the debate in the 2000s. For the roots of the debate see Schwartz (2004), 2057, footnotes 4 and 5; see also Rees (2013), 220.

[177] Purtova (2015), 3 et seq.

[178] Ibid., 8 et seq.

[179] Ibid., 11 et seq.

[180] Purtova (2010), 197, who also argues for a need of *de jure* allocation, because if there was no assignment *de jure*, *de facto* assignment is taking place anyway and property concentrates on the side of the more powerful actor (here: undertakings), see Purtova (2015); see also Marauhn / Thorn, (2013), para. 23 et seq.

[181] Purtova (2015), 2.

efficient level of privacy.[182] Indeed, the challenge is to develop a model for propertization, while at the same time safeguarding privacy.[183] This is reflected in economists' view of privacy, who mostly see it from a property rights perspective. They attach a two-sided function to property, since it contributes to both the protection of the fundamental right to privacy and the functioning of markets for personal data in the digital economy.[184] As the result would be property in information, parallels to intellectual property law can be drawn.[185]

However, leaving aside the practical **concerns** of introducing rights against the background of different national property regimes,[186] a more substantial counterpoint can be made: Property is based on the idea of alienability. Privacy, however, is a fundamental right (Art. 8 ECHR). There is a considerable debate amongst public law scholars over how to (re-)define the right to privacy and to what extent it can be waived, if it is conceived as a personality right.[187] Also, the interrelation with data protection law can cause confusion, and the extension of personal data protection to a property rights approach does have limits: The German Constitutional Court has explicitly stated that data protection laws protect informational self-determination. The Court explicitly noted that the individual does not and should not have absolute, unlimited sovereignty over his data. As personal data depict social reality, they cannot be allocated exclusively to an individual.[188] As a consequence, there is major hesitation in Germany to frame rights in personal data as property rights.[189]

Taking into account that personal data are information, **intellectual property** can inform according regulation. Especially the feature of inalienability calls to mind continental copyright regimes, based on the concept of moral rights, where the original right as such cannot be transferred. Accordingly, proposals have been made to introduce a copyright-like exclusive right to personal data.[190] However, the incentive argument, a cornerstone of copyright justification, does not apply to the production of personal data, as it is existent or created anyway. Also, the debate about the general justifications of copyright is still ongoing. This makes it hard to additionally accommodate personal data. Moreover, a parallel can be drawn to neighboring rights. In Germany, a new exclusive right for press publishers has been introduced.[191]

---

[182] Purtova (2010), 193 et seq.; Lessig (2002), 247.

[183] Schwartz (2004), 2058; see e.g. portability of personal data, which can basically be seen as an ownership right.

[184] Kerber (2016), 646.

[185] Ibid., 647.

[186] Purtova (2010), 199 et seq.

[187] Ibid., 203; Spieckermann / Acquisti / Böhme / Hui (2015), 162.

[188] BVerfG, Urteil v. 15.12.1983 – 1 BvR 209/83 (Volkszählungsurteil).

[189] Schwenke (2005), 71 et seq.

[190] Schwartmann / Hentsch, (2015), 226 et seq.

[191] The so-called "Leistungsschutzrecht für Presseverleger" was introduced in 2013 in §§ 87f-g of the German Copyright Act; currently, its introduction on the EU level is under discussion, see Art. 11 of the European Commission, COM(2016) 593 final, "Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market" of 14 September 2016.

This was a reaction to the problem that many business models benefit from the fact that publishers offer content for free on the Internet.[192] The law intends to grant revenues to publishers e.g. for news aggregation of third parties and to strengthen enforcement by allocating an absolute right.[193] There is some similarity to the data-as-property concept in the sense that a new property-like right was introduced for the dual purpose of control through economic participation and better enforcement. However, all neighboring rights require some performance on the part of the rights holder and—as opposed to personal data—not just a state of being.

So far, the property discussion has stayed—despite its length and depth—**purely academic**. Rather than proving actual power shifts, power theory offers an explanation for both why discussion about personal data property is tempting on the one hand and why no regulatory action has been taken in this regard on the other hand: Property-based approaches mainly seek to strengthen rights of data holders and empower individuals by granting an absolute right. But the respective normative justification is much more difficult than for justifying mere data protection rights.

As can be seen, property rights affect **all four dimensions of power**. While the control argument mostly strengthens relational power, the introduction of a property right has structural implications as well. A default allocation of exclusive rights—even when including exceptions—has significant impact on markets and privacy levels. However, it is too early to estimate the respective effects, and it seems questionable whether the market in fact works at all. Behavioral aspects (biases) especially can justify changing a default rule; however, they can also lead to market failure regarding re-allocation through transfers. Therefore, the introduction of a property right would most likely lead to complex and vast relational and structural power shifts which would be difficult, almost impossible to predict. For that reason, the issue can be seen as politically highly sensitive. Moreover, when the German Constitutional Court emphasizes that total exclusion would contravene the social function of personal data, it is basically stipulating a limitation of the power of data subjects.

3.5 Data Protection Law

3.5.1 Subject Matter

Data protection law[194] regulates the protection of natural persons (data subject) regarding the processing of their personal data. Data protection is recognized under Art. 16 TFEU and contributes to the protection of private life, which is a

[192] By systematic use, which reached beyond merely setting links.

[193] Jani (2014), para. 6.

[194] Dreier (2009), 44: "A certain convergence of private and public law can be observed in the area[…] of data protection – for the simple reason that the State no longer holds the monopoly in owning powerful data processing equipment which is capable of performing both mass data mining and individual profiling [...]."

fundamental right under Art. 8(1) ECHR. Data protection laws do not grant absolute rights in personal data, as the personality rights of the data subject are balanced against other fundamental rights.[195] However, their weight is high, considering that privacy—at least by the conception of German constitutional law—is an expression of personal freedom and human dignity.[196] As the GDPR stresses that it is also intended to contribute to the economic strengthening of the EU,[197] the regulation of personal data also has significant impact on the flow of personal data and therefore on business opportunities. However, even if data protection can be understood as "economic law" in that sense,[198] the core of data protection is to be understood as the regulation of privacy.

As a **legal source**, the GDPR is the general European framework for personal data protection. It is directly binding; however, the Member States have some discretion for adjustment of their national data protection laws. The GDPR touches on various issues related to personal data. Its creation has raised awareness of the interfaces of different legal areas. In addition, the ePrivacy Directive,[199] which is currently under revision, adds an additional layer of protection of basic rights in the electronic communication sector (e.g. cookies, tracking or anonymization), which the GDPR does not address precisely enough.

3.5.2 Data Protection from a Power Perspective

The processing of personal data poses mainly the type of risk that can be framed as a Weberian **causal-relational power concern**. As personal data by their very definition relate to an individual, "their use is likely to have an impact on a certain person's rights and interests".[200] Their processing can pose the risk of giving rise to discrimination, identity theft, fraud, financial loss, damage to reputation or other significant economic or social disadvantage[201] and therefore transfer power to the data controller. Once the link to the data subject is cut (e.g. through anonymization), relational power is divested.[202]

---

[195] Recital 4 GDPR.

[196] Marauhn / Thorn (2013), para. 28.

[197] Recital 2 GDPR.

[198] Schantz (2016), 1841.

[199] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy-Directive); see Commission Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications COM(2017) 10 final.

[200] See Art. 29 Working Party, Opinion 4/2007 on the concept of personal data, WP 136, 11.

[201] Recital 75 GDPR.

[202] Mayer-Schönberger / Padova, (2016), 329: "pseudonymization as means to divest power"; also as a means to reduce risk, see Rec. 28 GDPR.

Under the basic principle of data protection law, the processing of personal data is only legal, if it is permitted either by law or by consent of the data subject. While permission by law relates to considerations of public interest or balancing of private interests, the **data subject's consent** is a causal, individual power submission, which is the core of informational self-determination.[203] From a power perspective, this is similar to the mechanism of agreement as described in contract law, with the exception that consent is a unilateral exercise of free will. Due to the severe power consequences, the GDPR contains qualified requirements: Consent must consist in a clear affirmative act that establishes a freely given,[204] specific, informed[205] and unambiguous indication of the data subject's agreement to the processing of his data.[206] This is also the case for high-risk processing or treatment of personal data such as profiling.[207] In previous drafts, the GDPR excluded the possibility of voluntary consent where there is a clear imbalance between the parties.[208] However, this modal approach was not included in the final version of the GDPR.

Due to the high degree of power granted through giving access to personal data, the GDPR provides for several safeguards that enable the data subject to keep control over his data in a given relation by **limiting the controller's power**. In general, transparency requirements enable the data subject to effectively make use of his rights.[209] Three of these rights will be described in the following: First, the principle of purpose limitation (Art. 5(1) lit. b GDPR) requires that the processing is limited to the purpose for which the data is originally collected and processed. The purpose must be specific, explicit and legitimate and must be determined at the time of collection. This limits the controller's power significantly. While he can extend his power by defining a broad purpose beforehand or changing the purpose,[210] the higher requirements for consent limit this possibility.[211] Second, the principle of data minimization (Art. 5(1) lit. c) GDPR) dictates that personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which

[203] Of course, it is contested whether the theoretical conception holds true in reality. For a critical account on the role of consent (seen as "myth" or "misconception") see Blume (2014), 270; Koops (2014), 251 et seq.

[204] Not if clear imbalance (see Recital 43), but it is not entirely clear, when this shall be the case. Art 7(4) GDPR, extends to payment with data, see also Schantz (2016), 1845.

[205] Schantz (2016), 1844: Clearness of others (Art. 7(2) GDPR) comes close to the judicial control of standard terms as in consumer law.

[206] Recital 32 GDPR.

[207] But there must be explicit consent regarding profiling and safeguards might have to be established, see Art. 22, Art. 4 No. 4 GPDR, Recital 71 et seq.; see also Schantz (2016), 1844.

[208] Ex-Recital 34 named employment relationships as an example. However, this did not prevail in the final version of the GDPR.

[209] Art. 5(1) lit. a, Art. 12 GDPR: Rights to information and to access data in an intelligible form, see also Recital 39 GDPR on the prerequisites for the execution of rights.

[210] A change of purpose is possible under certain circumstances (Art. 6(4) GDPR), however, it is not clear yet where the limits are (in Germany, limits are usually tight, see § 28a BDSG), see also Kühling / Martini (2016), 451; Schantz (2016), 1844.

[211] Mayer-Schönberger / Padova (2016), 322 et seq.

they are processed. This clearly prevents the creation of relational power at least to a certain extent. Third, in general the data subject has the right to withdraw his consent and to claim deletion of the data.[212] Article 17 GDPR codifies this principle. As this has been discussed as "the right of being forgotten", it is actually nothing new to data protection principles. The GDPR just provides for a mechanism to effectuate this claim by also obliging those controllers who have published the information to inform other controllers.[213] The right to deletion is a relational disempowering mechanism.[214]

The newly introduced **portability right**[215] (Art. 20 GDPR) is of particular interest, due to its special power-related characteristics. Its basic idea is to enable individuals to transfer their personal data from one service to another without any hindrance (Art. 20(1) GDPR).[216] The GDPR also grants a right for direct transmission between data controllers on request of the data subject (Art. 20(2) GDPR). At first glance, this is in line with the relational power concept, as it is to prevent the data subject from consumer lock-in by granting more sovereignty over his "own" data.[217] While this disempowers the original data controller, the newly selected service gains power. However, the underlying reasoning is in fact based on a structural power assumption: The right to data portability targets services (data controllers) that have natural tendencies toward concentration through network effects, such as social networks, messengers etc. The consumer runs the risk of being locked in if switching costs are considerable.[218] By making it easier for him to move his data to another service, the right to data portability reduces his switching cost. As a consequence, market positions of the service providers become more contestable.[219] As can be seen, the legislature intends to foster competition between service providers and the opening of markets.[220] This poses two consequences: First, it is hoped that more competition will lead to an offer of a more diverse set of data protection standards and thereby further empower the consumer through a market mechanism.[221] In fact, this reasoning presumes a feedback loop of power—relational empowerment is used to change the structure, which in turn leads to greater relational empowerment of the data subject. Second, including a right to data portability in data protection law solves the modality problem as has been discussed in competition law (requirement of abusive causality), because it diffuses market power or

[212] Kühling / Martini (2016), 450.

[213] Recital 65 et seq.

[214] Frenz (2014), 194.

[215] European Data Protection Supervisor (2014a), para. 24 et seq.

[216] In general Swire / Lagos (2013).

[217] Geradin / Kuschewsky (2013), 9; Kühling / Martini (2016), 450; BT-Drs. 18/4721, 3.

[218] Picker (2008), 6 et seq.

[219] Monopolkommission (2015), Ch. 1 para. 62; Almunia (2012), 4.

[220] Kühling / Martini (2016), 450; Schantz (2016), 1845; European Data Protection Supervisor (2014a), para. 83.

[221] Kühling / Martini (2016), 450.

prevents its occurrence at an early stage.[222] While at first glance, the right to portability seems like a sensible solution, as it takes data protection and competition into account at the same time,[223] there is also some skepticism with regard to dynamic competitive effects[224] and potential identity fraud.[225] The future effects remain to be seen.[226] The analysis also implies that it is the unusual structural extension of the relational power paradigm of data protection law that has triggered some debate on interfaces of law.[227]

Data protection laws include provisions that also limit the possibility of consent. For **consent** to be valid, Art. 7(4) GDPR requires that the processing of the requested personal data is necessary for the performance of the contract. It is still not clear, however, how this is to be interpreted in practice. As Recital 43 refers to a "clear imbalance" between data subject and controller, one has to clarify whether this requires market power and therefore refers to a structural imbalance, or whether this merely refers to power in the bilateral relation between the parties.[228] The answer remains to be seen and has broad implications for the power understanding of the GDPR.

Another example related to consent is the case of sensitive data. Here, the law is based on the presumption that sensitive data merit special protection, because their processing could create significant risks to fundamental rights and freedoms.[229] In other words, the collection of these data can pose a significant relational power imbalance. Article 9 GDPR prohibits the processing of personal data that reveal e.g. racial origin, biometric data or sexual identity, unless the individual concerned has explicitly consented to it.[230] Moreover, the Member States can regulate that prohibition cannot be lifted by the data subject. This inalienability is based on a **modal power concept**, because the high risk is generally presumed for the particular type of data. The law eliminates any space for discretion attached to the will of the data subject, regardless of causality in a particular case. From this power perspective, data protection law has not only a causal-relational core, but also a modal branch.

---

[222] Of course, a breach of data portability obligations can constitute an abuse of dominance at the same time, Geradin / Kuschewsky (2013), 11; Schweitzer / Fetzer / Peitz (2016), 58.

[223] European Data Protection Supervisor (2014a), para. 72; Geradin / Kuschewsky (2013), 9 et seq.

[224] Swire / Lagos (2013), 338 et seq.

[225] Ibid., 339.

[226] Kühling / Martini (2016), 450; Ferretti (2014), 115.

[227] Specifically, the legislative proposal and implementation of data portability has triggered some overarching work: Rather holistic on different justifications for the right of data portability under Art. 20 (ex-Art. 18), Swire / Lagos (2013); with a competition focus Graef / Verschakelen / Valcke (2013); from a public law side see Fialová (2014), arguing with "more and less privacy".

[228] See Spindler (2016), 807, with further references for the proposed interpretations.

[229] Recital 51 GDPR.

[230] See also Recital 10 GDPR, employee data (Art. 88 GDPR); exemptions for health data have been crossed out; see Kühling / Martini (2016), 450, however, see also Recital 35 GDPR.

3.5.3 Implications

The extension of data protection laws to **structural power concerns** reflects the significant structural impact the mass processing of personal data in the digital world has. It is a reaction to the discussed shortcomings of competition law to account for structural power concerns in data protection laws. In this light it becomes clear why data protection and competition laws have lately developed a systemic interface and why the call for a regulation of personal data "under consideration of competition aspects" has been increasingly propagated.[231]

It is more difficult, however, to conclude that there is also a **tendency for modal extension**. The GDPR was primarily concerned with harmonization and has contributed to standardizing categories of sensitive data. However, as it leaves discretion to the Member States to entirely detach processing of sensitive data from personal consent, it can be expected that the definition of such modalities is likely to be a key task for national regulators. To a certain extent this corresponds with calls in the literature[232] to generally move away from notice and consent to regulating permissible and prohibited uses of personal data.[233] The underlying reasoning applies to such domains that are too complex for individuals to comprehend without expert knowledge and which have important negative externalities at the same time (e.g. food, drug and car safety).[234] Moreover, modal extensions of data protection law also explain on a theoretical level why data protection calls to mind consumer protection law and is often mentioned in comparison.[235] Also here, data protection regulation can compensate for some practical shortcomings of consumer protection regulation.[236]

3.6 Anti-Discrimination Law

In principle, **anti-discrimination laws** prohibit general discrimination in private relations e.g. on the basis of race, skin color, sex, language, religion, political or other views, national or social origin. But unequal treatment can be justified, if there is a legitimate reason (see also Art. 14 EHCR).[237] The jurisdictions of the Member

[231] Monopolkommission (2015), Ch. 1 para. 60; also European Data Protection Supervisor (2014a), para. 58 about using competition law for identifying breaches of data protection laws.

[232] Mayer-Schönberger / Padova (2016), 333, footnote 67 with further references, which say that this has not been implemented in the GDPR.

[233] Ibid., (2016), 332; see also the concept of contextualisiation by Nissenbaum (2010).

[234] Mayer-Schönberger / Padova (2016), 332.

[235] Kerber (2016), 643 et seq.

[236] Ibid.

[237] Cf. § 20 Allgemeines Gleichbehandlungsgesetz (AGG).

States have enacted substantial legislation and transposed European Directives[238] to tackle discrimination in a broad range of areas.

At their core, anti-discrimination laws follow a modal-relational power concept: They regulate the social relation between parties on grounds of defined circumstances.[239] Furthermore, the limits put to the freedom of contract are based on modalities, without the need to prove any causality.[240] But at the same time, non-discrimination laws can also be interpreted as following a **modal-structural power** approach. Renner argues that anti-discrimination laws imply the rationalization of private autonomy not only in individual relations, but also to society at large, as far as it intends to create a "culture of anti-discrimination".[241] From that perspective, non-discrimination laws reach out to influence the structure and are deliberately used to shape society. To put it in the words of Michel Foucault, subjects are constituted by internalizing norms and expectations of their information environment.[242]

Applied to personal data, the ongoing debate about the **role of algorithmic discrimination** deeply reflects respective power concerns.[243] Algorithms are sequences of instructions to execute a procedure. If decisions are based on algorithms, conscious or subconscious discrimination can take place. Social algorithms, in particular, result from the interaction with individuals. Two of the most prominent examples are Google's "Pagerank" and Facebook's newsfeed algorithm ("Edgerank"). The algorithm provides rules for the social network, and influences the agent's behavior or actions.[244] There is a growing debate in various jurisdictions on whether and to what extent algorithmic systems should be subject to regulation.[245] The normative challenge is to determine when measures like profiling and scoring violate constitutional rights.[246]

---

[238] Directive of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States; Council Directive of 27 November 2000 establishing a general framework for equal treatment in employment and occupation; Council Directive of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin.

[239] See §§ 19 et seq. AGG.

[240] See especially § 19(2) AGG.

[241] "Awareness of a culture of anti-discrimination", BT-Drs. 16/1780, 52; Renner (2016), 526.

[242] Hull (2015), 96.

[243] Hoffmann-Riem (2017).

[244] Tan (2007).

[245] See e.g. Executive Office of the President, May 2016, Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights. Also in Germany, the question of what a legitimate reason for justification of discrimination is, is very debated in the case of big data measures, especially scoring (§ 28b BDSG). The problem is that special rules in data protection laws exist, but they are bound to decisions related to contracts (therefore, not on behavioral targeting), see Schaar (2016), 33, with reference to § 28b BDSG. Also, it is not entirely clear if the GDPR accounts for that, see Goodman / Flaxman (2016), doing maximal and minimal interpretations and recognize a "right to explanation"; also the German Minister of Justice called for making search algorithms more transparent, see Dörr / Natt (2014), 838, footnote 68.

[246] Weichert (2014), 171; Schweitzer / Fetzer / Peitz (2016), 28, on the power related limits of profiling.

Algorithms based on personal data shift the respective social relation **from a causal to a modal power concept**. Schaar is concerned about the tendency for causal discrimination (e.g. methods to calculate individual risk as discrete measures), to turn into a modal paradigm once the discrimination is based on mere probability and not on certainty.[247] Even if the algorithm is fed by the behavior of data subjects, the distribution of power ultimately lies in the hand of the creator of the algorithm,[248] which is designed based on cultural perceptions about relevance and importance.[249] As a consequence, societal popularity even intensifies power.

But social algorithms also represent a shift **from a relational to a structural power concept**. This lies in the technical nature of the algorithm, which can be seen as a "structure" in this respect. What causes concern, rather than the power of an individual actor who knows "too much", is the power transferred to a system (the algorithm) to which we have already submitted personal information.[250] Therefore, power originates from the single relationships between the platform and the users, but is then transformed into structural power.[251]

It is the combination of modal and structural power aspects that illustrates that the discriminatory power of (social) algorithms has broad power implications, which can be fit under Foucault's concept of power. There is already some literature which explicitly applies his work to social algorithms. Framed in Foucault's terms, subjects are not autonomous and exogenous to their information environment.[252] Algorithms function as a disciplinary technique that creates subjects who endlessly modify their behavior to approximate the normal.[253] Subjects are partly shaped by their information environment and choices about whether to surrender personal data will become a part of society's individuals.[254] At the same time, scoring illustrates the much broader concern that choices made by computers may prevail over the personality rights of human beings,[255] which could lead to the computerized algorithm holding the power to **organize society**. Basically the individual users are remodeling themselves through a structural mechanism and society is becoming transformed as a consequence.[256] It remains to be seen if the "culture of anti-discrimination" the German legislature referred to when transposing the respective EU Directives will prevail over the tremendous modal-structural power implications of (social) algorithms, which—at first glance—rather appear to create a general

[247] Schaar (2016), 27 et seq.; Weichert (2014), 170: plausibility is enough.

[248] Even if users contribute to the algorithm to learn.

[249] Bucher (2012), 1167.

[250] Ibid., 1171 et seq., thus following a non-relational power-perception.

[251] Ibid.

[252] Hull (2015), 96.

[253] Bucher (2012), 1176.

[254] Hull (2015), 96.

[255] Weichert (2014), 170.

[256] Hull (2015), 98.

"culture of discrimination" on a large scale.[257] However, these general tendencies are very difficult to tackle by law in general and in particular by private law.

3.7 Going Beyond: Power of Opinion as a Subject of Media Regulation

Media regulation can add to a more refined delineation of modal-structural power implications and the law with respect to the use of personal data. Though media regulation lies beyond private law, a short discussion seems necessary, as it helps to identify the limits of power considerations that can be accommodated in regulatory approaches under private law. Algorithmic discrimination is an illustrative example of the modal-structural power dimension of personal data. But its impact reaches beyond the mere decentral, relational organization of individuals. As Lazer states, "the rise of the social algorithm" is a "quiet but epic paradigm shift" which is "fraught with social and policy implications".[258] The main concern is the influence of social algorithm-based networks on **shaping public opinion**. In particular, this addresses the concern that data power constitutes the power to influence opinions and thereby grant political power.[259] Search engines also bear a high potential of risk in this respect because of their role and systemic capability to shape opinions.[260] Economic incentives lead to the result that algorithms are based on relevance and not on diversity.[261]

In Germany there is especially strong media **regulation**, which is based on the following assumption: Once a broadcaster's content becomes popular to an extent that constitutes power of opinion ("Meinungsmacht"), it is subject to special obligations to guarantee that diverse opinions are expressed and that comprehensive information is offered.[262] This follows the underlying premise that if there are no safeguards against private power of opinion, public opinion will be shaped in an irreversible way. This means that it would be impossible to restore media diversity—and therefore a plurality of opinions, which is seminal for a working democracy. It becomes evident that there are good reasons for a dedicated public debate about whether to extent media regulation to influential, algorithm-based Internet platforms.[263] Their common core lies in a modal-structural power concern.

---

[257] Bauman / Lyon (2013), 52 et seq., on social exclusion through "surveillance techniques" like profiling.

[258] Lazer (2015), 1090.

[259] Schweitzer / Fetzer / Peitz (2016), 29.

[260] Dörr / Natt (2014), 832.

[261] Ibid., 835.

[262] §§ 25, 26 RStV, see Dörr / Natt (2014), 840, elaborating on the constitutional reasons (BVerfGE 57, 295, 320; 119, 181, 214).

[263] Dörr / Natt (2014), 846; recently Drexl (2016).

4 Findings and Implications

4.1 Towards a Holistic Approach

The **power paradigm** underlying these areas of law serves as a common denominator on a higher level, due to its individual and societal significance for the processing of personal data. The previous discussion of power concepts in private law has revealed that the power paradigm makes it possible to link the related areas in regulating personal data. Therefore, the power paradigm can serve as theory-based guidance for the legislature to create both effective and coherent regulation. The most general insight is that personal data is indeed relevant in many areas of private law. Also, all of the power concepts described have proven to be significant in regulating personal data. As a result, the regulation of personal data is challenging and highly complex. The power paradigm approach structures this complexity by distinguishing between four different concepts of power, which in turn correlate on a more abstract level. By identifying the abstract power interrelations, one can gain a better understanding of the individual interrelations in the various areas of private law. In particular, it has been shown that:

- Contract law is causal-relational in its core, but is nowadays also deliberately used for targeting structural power concerns involving personal data.
- Consumer law is modal and increasingly used for personal data issues.
- Competition law follows a structural concept and—for that reason—is heavily discussed and applied in practice. Its causal core assumption is questioned by some advocates, who intend to accommodate modal power concerns as well.
- Property law has implications for all power dimensions and is discussed in the literature. However, it is not of significant relevance for practice.
- Data protection law is relational and has causal as well as modal elements. The modalities are currently being re-configured by regulators, while data protection law nowadays also considers structural power considerations.
- Anti-discrimination law is based on a modal-relational concept, but has structural-modal implications as well. For that reason it will certainly become more important in the near future against the background of "big data" activities.

The recent developments in digital processing of personal data have significantly changed power balances. The power-related challenges are different by their nature, as shown by the application of the private power taxonomy. In consequence, different areas of private law tackle different sorts of challenges. However, since a single area can already address more than one power concern, significant overlaps occur. In addition, convergence can be observed, due to the fact that regulation has shifted in various areas of private law. In particular, a shift from causal to modal as well as from relational to structural power perceptions is taking place.

But what are the **implications** of this analysis? This study has identified descriptive implications (discussed under Sect. 4.2), which can be structured into three different levels: the "micro-level" regarding the specific areas of law, the "meso-level"

regarding the power implications for holistic regulation and the "macro-level" for power theory itself. Subsequently, the normative implications of the analysis are to be discussed (under Sect. 4.3). Though the study has identified and observed the occurrence and framing of power, it has not yet elaborated on the prescriptive question to what extent regulation should consider private power as legitimate or distribute it. The theory of private power gives some abstract answers, which can be discussed with respect to personal data. However, this will only be done briefly, as a thorough discussion goes far beyond what can be accomplished in this frame.

4.2 Descriptive Findings and Implications

4.2.1 Micro-Level: Changes in Areas of Law

Obviously, the occurrence of personal data challenges various areas of private law. Many of these areas have undergone transition or are still being further elaborated, regardless of personal data. Therefore, personal data issues **encounter ongoing legal debates**, such as the European harmonization of sales contract law, the effectuation of enforcement regimes, the normative refinement of competition law or the debate on justifications concerning intellectual property rights (especially neighboring rights). This adds further complexity to the current discussions relating to the regulation of personal data.

At the same time, the above-mentioned legislative measures illustrate that personal data-related problems materially contribute to the **general re-configuration of legal areas**: Contract and data protection law emphasize the role of agreement/consent. By recognizing personal data as non-monetary consideration the position of the data holder is strengthened. The legal status of the data holder is readjusted to the *actual* situation. At the same time, the chosen legal construction basically conceptualizes the provision of data as a long-term obligation, rather than a spot contract. Legislation mainly addresses consumers and consumer protection law is also discussed from a more general angle (e.g. what are normative imbalances of power in consumer law[264]) and used to correct enforcement deficits of other areas of law. While so far there is only an academic debate about personal data from an intellectual property point of view, competition law discusses the suitability of given standards for personal data. But it also questions the standards as such, e.g. whether the goal of the law itself should account for privacy as consumer welfare or how markets for personal data can be constituted or whether they work at all. All of these examples show that personal data contributes to a general dynamic in reconsidering established areas of private law.

[264] Renner (2016), 507.

4.2.2 Meso-Level: Power and Regulation

4.2.2.1 Observations on the Concepts of Power

The analysis reveals that the power taxonomy has significant value for explaining the reasons and the methods of regulating personal data in private law. First, the examination of personal data in private law shows that the power concepts described above are **linked in several ways**. These links have to be carefully observed and disentangled. There is a *cumulative* link, as it has been shown that different areas of private law either already touch upon different power concepts (property law being the most illustrative one) or solve personal data-related problems by extending other power concepts. Extension in that sense does not mean a substitution, but can be understood—depending on the conventional power reasoning of the legal area—as a shift. The *chronological* link between different power concepts is nicely illustrated by the feedback loop of data portability. In this context, relational empowerment is used to change the structure (here: market), which then again leads to more relational empowerment of the data subject.

Second, the taxonomy provides an analytical tool that has enabled the identification of ongoing **shifts** in private law. These shifts are reflected in the power concepts and have been triggered by the mass processing and commercialization of personal data. In particular, the taxonomy helps us to understand which power concepts have gained significance under what circumstances. This explains at a practical level why particular interfaces between different legal disciplines have significantly gained attention. At the same time, it also points to the struggle of finding holistic, coherent regulatory concepts. As a result, the quality of power has continuously extended towards modal and structural forms of power, which the legislature has increasingly taken into account. More and more regulation accounts for structural aspects of personal data—sometimes more, sometimes less explicitly. Competition law is the main framework for regulating a form of structural power. As the importance of data processing has increased and consequently new markets have been created and reshaped, it does not come as a surprise that the debate on the impact of personal data on competition law and respective regulatory measures are highly visible these days. Rather, it is surprising that the amendment of consumer contract law is also based on the logic of systemic market correction and therefore takes structural considerations into account. Moreover, the introduction of portability is untypical for data protection frameworks, which are conventionally concerned about relational and not structural power. At the same time, private law increasingly shifts towards a modal understanding when regulating personal data. Consumer contract law is on its way to explicitly recognize data as counter-performance and grants certain rights to consumers, based on the implicit assumption of a general power imbalance, which is, however, not related to personal data in particular.[265] In competition law,

[265] Also shows that it shifts conventional power conceptions of the legal fields, so it triggers a debate about the extremes of the legal fields and therefore also develops the fields as such (see e.g. Faust (2016)).

the debate on whether causal considerations should be detached and on whether modalities should be defined instead, is an old regular. It re-triggers familiar discussions, such as whether dominance as such can be harmful and if so whether there is a call for regulation. Data protection law is still consent-focused and therefore causality based. However, the GDPR leaves discretion to the Member States to introduce special rules, which enables them to shift away from causal towards modal power concepts.

Third, the automated mass processing of personal data has led to new phenomena of structural power. **Social algorithms** enable private actors to execute significant private power, not only on individuals, but on entire structures, such as shaping public opinion or creating a civil society of discrimination. Their mechanisms and significance have been increasingly debated over the last few years and more concrete calls for regulation are currently being discussed.

4.2.2.2 Implications for Regulation

Based on these observations, a couple of conclusions for regulation can be drawn. Without any doubt, private law is a determining factor for the allocation of power. But the **complex concept** of power implies that it would be too simple to merely claim "consumer sovereignty" or "empowerment" as a solution to the challenges.[266] In general, there are different kinds of power control, such as procedural control, result control or neutralization.[267] The regulation of personal data can and should make use of all of them. Regulatory intervention must be both prudent and analytic, because due to the complexity of the subject-matter, unintended side-effects are likely to occur.

Power theory serves as a tool which can help to **order** the problems related to personal data when thinking about how to regulate. As a *first step*, particular situations of the processing of personal data can be observed with respect to their power implications and allocated to the taxonomy accordingly. One must be aware that this study only refers to ideal-typical dichotomies (causal-modal and relational-structural). Of course, more specific analysis can examine the spectrum of these two power dimensions in a more granular fashion. As a *second step*, the links of the power implications can be carved out. This study gives some hints about general shifts and interrelations and it will need to be seen whether they hold true in each particular case. It is obvious that there is a need for empirical research. As a *third step*, reference can be made back to the different legal areas and—taking into account their conventional power perception—it can be seen how the findings of the power analysis affect different areas of law. For example, one can observe how strong the presumption of causality in the respective area is (e.g. strong causality,

[266] This reminds of Galbraith, who coined the theory of counter-power, as one sort of solution to the problem, see Schweitzer (2016), 472. One has to analyze, if such a constellation is given in case of personal data power.

[267] Kainer / Schweitzer (2016), 639 et seq.

(un-)rebuttable presumption) or what particular criteria for modalities apply. This power-guided approach has the advantage of tackling the particular problem in a more analytical, but also in a more systematic way. The approach is holistic, since it does not limit solutions to certain legal areas or their interfaces beforehand and lays the groundwork for an ultimately more coherent normative reasoning.

Private law has considerable experience in dealing with causal-relational power, to some extent with causal-structural power, and in recent decades with modal-relational power as well. However, it struggles to deal with **modal-structural power**. There is an evolutionary explanation for this: Private law considered structural power long before it also recognized modal power. The power evolution of personal data, however, has worked the other way round. While the modal concept of "sensitive data" has existed for a long time, only lately has the processing of such data made a significant structural impact. This evolutionary lack of experience for private law poses new challenges for the legislature. Even more importantly, there is a material reason for the challenge the modal-structural power concept of personal data poses for private law: Due to its structural quality, modal-structural power constellations have significant societal implications. However, because of the lack of immediate causality, the (assumed) circumstances and reasons for their impact are just as important as they are difficult to define. Power theory gives a good explanation for why it is even more necessary for the regulator to approach such problems and to put prudent efforts into defining structures and modalities that evolve and shape the individuals as a consequence. There is a remarkable parallel: While algorithmic decision-making refers to a structure (the algorithm) and is based on assumptions rather than on causalities, legislative approaches to domesticate these problems tend to follow the same structural-modal patterns. To define the modalities, empirical work is needed and ethical reasoning is indispensable for making a regulatory choice. The example of social discrimination in algorithms and media regulation show that usually such implications go beyond the terrain of private law. Solutions will then fall within the domain of public law.

4.2.3 Macro-Level: Power Theory

Three goals have been achieved by this study:

First, on a theoretical level, it has been shown that the framework of private power serves as a workable descriptive theory which can be applied to the regulation of **personal data** in private law and even beyond that. The truism "knowledge is power" is relevant for drafting regulation, but in this study, it has been further refined and differentiated into a tool that can translate personal data into workable legal terms.

But secondly, it can also be observed that personal data contribute to the **power theory itself**: This study has introduced a dynamic factor by elaborating on the power shifts to which particular areas in private law are exposed when regulating personal data. Thus, the theory itself has been more refined, as it systematically observes the legal relevance of linkages and development paths.

Third, personal data have revealed different means of power distribution and disempowerment due to the informational nature of the subject being observed. Therefore, they contribute to a **general theory of power** related to information in private law.

4.3 Normative Implications

4.3.1 Normative Yardstick for Regulatory Intervention

Normative implications cannot be derived automatically from the power theories because they require a decision paradigm (usually value judgments or political considerations), which has to be deliberately chosen. Therefore, power imbalances cannot be regarded as inherently good or bad. Rather, the normative evaluation of power depends on the specific context. Backed up by experience, however, private law has a differentiated scheme on what sorts and degrees of power are to be considered as unjust or necessary in a given reference system. The crucial question for regulators is what form of power needs regulation under what circumstances.

As a general rule of thumb, those sorts of power are especially troublesome—by liberal standards, but also under stability and legitimacy considerations[268]— that define unilateral scopes of action that are (potentially) harmful to systems that constitute the scope of actions under concrete circumstances.[269] From a legal perspective, normative implications can be categorized into two different groups when setting **limitations to power**. First, one can determine the immanent limits of action for the individual that must be preserved in order to keep a freedom-based reference system viable.[270] Second, one can define the external limits of the system, based on value judgments. This distinction tries to draw a clear line between law and policy considerations, and it can justify as well as explain policy considerations.

The main normative implication for legal scholars is that they should primarily **focus on determining the immanent limits** of an individual's actions which must be preserved to keep the reference system functioning. When evaluating power, regulators should be aware of the types and the intensity of power control as well as the suitable level of regulation. If an effect causes irreversible damage to the functioning of the respective reference system, regulatory action is definitely necessary. This should also be the case if this damage is likely and/or if the intensity of the

[268] See Bachmann (2016) for a comprehensive treatment of the legitimation of private power, taking a broader perspective on approaches under which private power can be justified and discussing source, sort and consequences of power as determinants for justification in particular, 616 et seq.

[269] Ibid., 630.

[270] Ibid.

power in question is high.[271] It is just as important to determine the external limits of the system. However, those limits are based on value judgments which should be debated in the political forum.

4.3.2 Implications for Regulating Personal Data

What can be said about the internal limitations to power with respect to various areas of private law? For the concept of power, the legislative context or the **relevant reference system** must be decisive.[272] The establishment of what type of power is in need of regulation follows different principles in the respective systems.[273] Usually the respective concept of power corresponds to the actual functional conditions of the system (e.g. private/autonomous self-organization in contract law; free competition and the market in competition law; non-discriminatory culture in anti-discrimination law etc.).[274] In this respect, there is no such thing as general under- or overregulation.[275] Also, the problems cannot be reduced to the idea of informational self-determination, even though in general, constitutional law is obviously the prime legal source for normative guidance when determining the outer limits in different areas of private law.[276]

As shown, a fundamental characteristic of personal data issues is that they affect several areas of private law and different power concepts. Therefore, the question of internal limitations to power must be answered separately in each individual area. At the same time, however, one must also take into account the strong underlying links and interrelations. As an **example, personal price discrimination**, based on profiling and behavioral tracking, can illustrate how the power taxonomy can structure the problem in a way that helps to identify the neuralgic point for determining normative, internal limitations. Let us take the simple case that a service provider offers users individual prices based on permanent tracking and analysis of the user's behavior (e.g. a flight is offered to a particular user for a higher price, because from the user's tracked behavior, it seems likely that he urgently needs to book the flight). If the processing of personal data for this purpose is based on the consent of the

[271] Ibid., 636 et seq.; Bäcker (2012), 106, 108.

[272] Kainer / Schweitzer (2016), 630.

[273] Ibid., 630.

[274] Ibid., 632.

[275] See Kerber (2016), 646 et seq., who admits that even with rather holistic approaches, things are so complex that a lot of regulatory errors are to be expected, both in regard to under- and overregulation. For a comprehensive elaboration on the relationship between power, private law and economics, see Käseberg (2016), who concludes that economics cannot (yet) explain issues which are seminal for private law in general and for power issues in particular and can therefore only deliver solutions with limited reach (at 600). When reconciling his conclusion with the findings of this study, it becomes obvious that the ubiquitous relevance of power for personal data also implies the limited usefulness of economic analysis as a paradigm for regulation.

[276] See Calliess (2006), para. 6, stating that the density of control is not entirely clear when it comes to matters of private power.

user, contract and data protection law will inquire into the causal-relational power balance and observe whether informed consent is in fact possible on these terms. These areas of law will also raise the question whether a shift to a modal understanding might disallow for consent. This is relevant for those cases where an inherent power imbalance between the parties is assumed and such a practice can have severe consequences for the private (informational) autonomy of the individual. But moreover, internal limits can be reached, due to causal-structural power implications. Individualized price discrimination based on algorithms can pose a serious risk to the functioning of entire markets, as the ex-ante discretion of the buyers' reservation price is a fundamental implicit assumption. Finally, a modal-structural implication is that individual price discrimination can create a general culture of social discrimination. It becomes obvious that the multiple power implications involved in the issue of personal profile-based price discrimination require a holistic analysis, before finding solutions in different areas of law. It would be insufficient to say that, for example, increased transparency in contract law would solve the problem. The problem is much more complex and needs empirical evidence for determining limits and solutions.

Finally, it needs to be clear when internal limitations are affected, and when, in fact, external limitations are relevant. Determining these **external limitations** requires value judgments and public discourse, which should be both passionate and constructive. Much seems to be at stake, considering that the processing of personal data nowadays not only goes to the core of personal self-determination and private autonomy, but also affects markets and public opinions and eventually transforms society and culture. The fact that internal limitations in an area of law are not exceeded does not preclude the need for an adjustment of external limitations. Therefore, lawyers must understand and tolerate changes of paradigm in their respective legal areas as a small contribution (or sacrifice) to the benefit of society at large.

5 Summary

1. A holistic approach regarding the regulation of personal data in private law is both lacking and needed. Power can serve as the paradigm to enable the construction of a holistic approach by linking different areas of private law on a higher level of abstraction. This theory-based approach allows for a coherent and prudent regulation of personal data in the future.
2. Power is a subject of sociology and philosophy, rather than an explicit matter of legal scholarship. Various concepts of power exist. Based on the findings of F. Möslein et al. (2016), four concepts of power can be identified that are of special importance for private law, namely causal-relational (Weber), causal-structural (Eucken), modal-relational (Luhmann) and modal-structural (Foucault) forms of power. These power concepts are also reflected in those areas of private law that can be identified as most relevant for the regulation of personal data: the

law of contract, consumer protection, competition, (intellectual) property, data protection and anti-discrimination.

3. The power-focused analysis of the current regulation of personal data through private law reveals the following: Contract law is causal-relational in its core, but is nowadays also deliberately used for targeting structural power concerns involving personal data. Consumer law is modal and increasingly used for personal data issues. Competition law follows a structural concept and—for that reason—is heavily discussed and applied in practice. Also, some advocates question its purely causal assumption and intend to accommodate modal power concerns as well. Property law has implications for all power dimensions and is discussed in the literature. However, it is not of significant relevance for practice. Data protection law is relational by its very conception and has causal as well as modal elements. The modalities are currently being re-configured by regulators, while at the same time, data protection law nowadays also considers structural forms of power. Anti-discrimination law is based on a modal-relational concept, but has structural-modal implications as well. For this reason, it will certainly become more important in the near future against the background of "big data" activities.
4. The areas of law themselves have been re-configured due to the relational effects and the significant societal impact of the processing of personal data. Therefore, a convergence between the areas can be observed, while regulation moves or extends from causal to modal and from relational to structural power perceptions.
5. Prudent holistic regulation of personal data can progress in the following order: As a first step, particular situations of the processing of personal data can be observed with respect to their power implications and allocated to the taxonomy accordingly. As a second step, the links of the power implications can be traced. This study gives some hints about general shifts and interrelations and it needs to be seen in the particular case whether they hold true. Empirical support is necessary for decision-making. As a third step, reference can be made back to the different legal areas—taking into account their conventional power perception—to see how the findings of the power analysis affect different areas of law. This power-guided approach has the advantage of tackling the particular problem in a more analytic, but also in a more systematic way. This might ultimately lead to effective and coherent regulation of personal data.
6. The holistic approach sets the stage for finally establishing a more coherent structure of normative reasoning. However, there is no universal normative answer, since power imbalances cannot be regarded as inherently good or bad. Rather, the normative evaluation of power depends on the specific context. One can distinguish between two decision paradigms for setting limits to power: First, one can determine the immanent limits for action of the individual, which must be preserved in order to protect the viability of a freedom-based system. Second, one can determine the external limits of the respective system, based on value judgments. This distinction draws a clear line between law and policy considerations.

References

Abrahamson, Z.G. (2014), Essential Data, 124 The Yale Law Journal 867

Ackermann, T. / Franck, J.-U. (2014), Chapter 4: Validity, in European Contract Law and German Law, in: S. Leible / M. Lehmann (Eds.), European Contract Law and German Law, 167, Wolters Kluwer

Acquisti, A. / Taylor, C. / Wagman, L. (2016), The Economics of Privacy, 52 Journal of Economic Literature 442

Almunia, J. (2012), Competition and personal data protection, SPEECH/12/860, 26 November 2012, available at: http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm

Armbrüster, C. (2015), § 138 BGB Sittenwidriges Rechtsgeschäft, in: F.-J. Säcker / R. Rixecker / H. Oetker / B. Limperg (Eds.), Münchener Kommentar zum Bürgerlichen Gesetzbuch, 7th ed., C.H.Beck

Bachmann, G. (2016), Die Legitimation privater Macht, in: F. Möslein (Ed.), Private Macht, 603, Mohr Siebeck

Bäcker, M. (2012), Grundrechtlicher Informationsschutz gegen Private, 51 Der Staat 91

Basedow, J. (2007), Konsumentenwohlfahrt und Effizienz – Neue Leitbilder der Wettbewerbspolitik?, 57 Wirtschaft und Wettbewerb 712

Bauman, Z. / Lyon, D. (2013), Liquid Surveillance, Polity Press

Behrens, P. (2015), The Ordoliberal Concept of 'Abuse' of a Dominant Position and its Impact on Article 102 TFEU, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2658045

Berger, J. (2016), Macht als Grundbegriff der Soziologie, in: F. Möslein (Ed.), Private Macht, 47, Mohr Siebeck

Blume, P. (2014), The myths pertaining to the proposed General Data Protection Regulation, 4 International Data Privacy Law 269

Böhm, F. (1960), Das Problem der Privaten Macht – 1928, in: E.-J. Mestmäcker (Ed.), Franz Böhm – Reden und Schriften, 25, C.F. Müller

Bräutigam, P. / von Sonnleithner, B. (2015), Vertragliche Aspekte der Social Media, in: G. Hornung / R. Müller-Terpitz (Eds.), Rechtshandbuch Social Media, 35, Springer

Bucher, T. (2012), Want to be on the top? Algorithmic power and the threat of invisibility on Facebook, 14 New Media & Society 1164

Buchner, B. (2006), Informationelle Selbstbestimmung im Privatrecht, Mohr Siebeck

Buchner, B. (2008), Wissen ist Macht? Zum Verhältnis zwischen Datenschutz und Wettbewerb, 32 Datenschutz und Datensicherheit 724

Bundeskartellamt (2016), Arbeitspapier Marktmacht von Plattformen und Netzwerken, B6-113/15 of June 2016, available at: www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Think-Tank-Bericht.html?nn=3591568

Calliess, G.-P. (2016), Private Macht und Verbraucherrecht, in: F. Möslein (Ed.), Private Macht, 213, Mohr Siebeck

Calliess, C. (2006), § 44 Schutzpflichten, in: D. Merten / H.-J. Papier (Eds.), Handbuch der Grundrechte in Deutschland und Europa, Vol. 2, 963, C.F. Müller

Canaris, C.-W. (2000), Wandlungen des Schuldvertragsrechts – Tendenzen zu seiner "Materialisierung", Archiv für die civilistische Praxis, 273, Mohr Siebeck

Cashin Ritaine, E. (2012), Common Frame of Reference and Property Law: A General Introduction, in: S. v. Erp / A. Salomons / B. Akkermans (Eds.), The Future of European Property Law, Sellier

Competition and Markets Authority (2015), The Commercial use of consumer data, available at: www.gov.uk/cma-cases/commercial-use-of-consumer-data

Cohen, J.E. (2012), Configuring the Networked Self – Law, Code, and the Play of Everyday Practice, Yale University Press

Cohen, J.E. (2013), What Privacy Is For, 127 Harvard Law Review 1904

Cooper, J. (2013), Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity, 20 George Mason Law Review 1129

Dietrich, F. / Ziegelmayer, D. (2013), Facebook's "Sponsored Stories" – ein personenbezogenes unlauteres Vergnügen, 29 Computer & Recht 104

Dörr, D. / Natt, A. (2014), Suchmaschinen und Meinungsvielfalt, 58 Zeitschrift für Urheber- und Medienrecht 829

Dreier, T. (2009), Regulating Information: Some thoughts on a perhaps not quite so new way of looking at intellectual property, in: J. Drexl / R.M. Hilty / L. Boy / C. Godt / B. Remiche (Eds.), Technology and Competition – Technologie et concurrence, Contributions in Honor of Hanns Ullrich, 35, Larcier

Drexl, J. (2011), On the (a)political character of the economic approach to competition law, in: J. Drexl / W. Kerber / R. Podszun (Eds.), Competition Policy and the Economic Approach, 312, Edward Elgar

Drexl, J. (2016), Was dem Leser gefällt!, Süddeutsche Zeitung of 4 September 2016, available at: www.sueddeutsche.de/wirtschaft/forum-was-dem-leser-gefaellt-1.3147503

Drexl, J. / Hilty, R.M. / Greiner, F. / Kim, D. / Richter, H. / Surblytė, G. / Wiedemann, K. (2016), Ausschließlichkeits- und Zugangsrechte an Daten, 65 GRUR Int. 914

European Data Protection Supervisor (2014a), Preliminary Opinion of the European Data Protection Supervisor, Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, March 2014, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf

European Data Protection Supervisor (2014b), Report of workshop on Privacy, Consumers, Competition and Big Data, 2 June, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Big%20data/14-07-11_EDPS_Report_Workshop_Big_data_EN.pdf

European Data Protection Supervisor (2016), Opinion 8/2016 of the European Data Protection Supervisor on coherent enforcement of fundamental rights in the age of big data, of 23 September 2016, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Events/16-09-23_BigData_opinion_EN.pdf

Eucken, W. (1965), Die Grundlagen der Nationalökonomie, Springer

Evans, D.S. (2011), The Antitrust Economics of Free, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1813193

Faust, F. (2016), Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update? Gutachten zum 71. Deutschen Juristentag, available at: http://www.djt.de/fileadmin/downloads/71/fachprogramm/djt_71_Zivilrecht_160408.pdf

Ferretti, F. (2014), EU Competition Law, the Consumer Interest and Data Protection – The Exchange of Consumer Information in the Retail Financial Sector, Springer

Fialová, E. (2014), Data Portability and Informational Self-Determination, 8 Marsaryk University Journal of Law and Technology 45

Foucault, M. (1976), Mikrophysik der Macht, Merve Verlag

Foucault, M. (2015), Analytik der Macht, 6th ed., Suhrkamp

Franck, J.-U. (2016), Eine Frage des Zusammenhangs: Marktbeherrschungsmissbrauch durch rechtswidrige Konditionen, 14 Zeitschrift für Wettbewerbsrecht 137

Franz, B. / Podszun, R. (2015), Was ist ein Markt? – Unentgeltliche Leistungsbeziehungen im Kartellrecht, 3 Neue Zeitschrift für Kartellrecht 121

Frenz, W. (2014), Datenschutz durch Kartellrecht, 5 Europäisches Wirtschafts- und Steuerrecht 193

Geradin, D. / Kuschewsky, M. (2013), Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2216088

Goodman, B. / Flaxman, S. (2016), European Union regulations on algorithmic decision-making and a "right to exploitation", available at: https://arxiv.org/abs/1606.08813

Graef, I. / Verschakelen, J. / Valcke, P. (2013), Putting the Right to Data Portability into a Competition Law Perspective, The Journal of the Higher School of Economics Annual Review 53

Han, B.-C. (2005), Was ist Macht?, Reclam
Hanau, H. (2016), Die Schranken privater Gestaltungsmacht – Zur Herleitung einer Angemessenheitskontrolle aus den Grenzen der Selbstbindung, in: F. Möslein (Ed.), Private Macht, 119, Mohr Siebeck
Harbour, P.J. /Koslov, T. (2010), Section 2 in a Web 2.0 world: An expanded vision of relevant product markets, 77 Antitrust Law Journal 769
Hauer, M. / Rudkowski, L. / Goren, P. / Lahr, M. / Oestreich, J. / Renner, M. / Schmidt, S. / Schreiber, A. (2013), Macht im Zivilrecht, Boorberg
Heller, C. (2011), Post-Privacy, C.H.Beck
Hellwig, M. (2006), Effizienz oder Wettbewerbsfreiheit? Zur normativen Grundlegung der Wettbewerbspolitik, in: C. Engel / W. Möschel (Eds.), Recht und spontane Ordnung: Festschrift für Ernst-Joachim Mestmäcker zum achtzigsten Geburtstag, 231, Nomos
Henning-Bodewig, F. / Spengler, A. (2016), Conference Report: "Framing – The 'Hard Core' of Unfair Competition Law, 65 GRUR Int. 911
Herresthal, C. (2016), Private Macht im Vertragsrecht – Austauschverträge, in: F. Möslein (Ed.), Private Macht, 145, Mohr Siebeck
Hoffmann-Riem, W. (1998), Informationelle Selbstbestimmung in der Informationsgesellschaft, 123 Archiv des öffentlichen Rechts 513
Hoffmann-Riem, W. (2017), Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht, 142 Archiv des öffentlichen Rechts 1
Hoofnagle, C.J. / Whittington, J. (2014), Free Accounting for the Costs of the Internet's Most Popular Price, 61 UCLA Law Review 606
Hull, G. (2015), Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data, 17 Ethics Inf Technol 89
Jani, O. (2014), § 87f UrhG Presseverleger, in: A.-A. Wandtke / W. Bullinger (Eds.), Praxiskommentar zum Urheberrecht, 4th ed., C.H.Beck
Kainer, F. / Schweitzer, H. (2016), Ansätze für eine Systematisierung von privater Macht und der Begrenzung privatrechtlicher Gestaltungsmacht, in: F. Möslein (Ed.), Private Macht, 629, Mohr Siebeck
Käseberg, T. (2016), Macht, Privatrecht und Ökonomik – Nutzen und Grenzen der Ökonomik bei der Analyse privater Macht im Privatrecht, in: F. Möslein (Ed.), Private Macht, 581, Mohr Siebeck
Kerber, W. (2016), Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection, 65 GRUR Int. 639
Köhler, H. (2015), § 1 UWG, in: H. Köhler / J. Bornkamm (Eds.), Gesetz gegen den unlauteren Wettbewerb, 33rd ed., C.H.Beck
Koops, B.-J. (2014), The trouble with European data protection law, 4 International Data Privacy Law 250
Körber, T. (2016a), "Ist Wissen Marktmacht?" Überlegungen zum Verhältnis von Datenschutz, "Datenmacht" und Kartellrecht – Teil 1, 4 Neue Zeitschrift für Kartellrecht 303
Körber, T. (2016b), "Ist Wissen Marktmacht?" Überlegungen zum Verhältnis von Datenschutz, "Datenmacht" und Kartellrecht – Teil 2, 4 Neue Zeitschrift für Kartellrecht 348
Kühling, J. / Martini, M. (2016), Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, 27 Europäische Zeitschrift für Wirtschaftsrecht 448
Kuschewsky, M. / Geradin, D. (2014), Data Protection in the Context of Competition Law Investigations: An Overview of the Challenges, 37 World Competition Law and Economic Review 69
Langhanke, C. / Schmidt-Kessel, M. (2015), Consumer Data as Consideration, 1 Journal of European Consumer and Market Law 218
Lazer, D. (2015), The rise of the social algorithm, 348 Science 6239
Lehmann, M. (2016), Private Macht im Eigentumsrecht, in: F. Möslein (Ed.), Private Macht, 281, Mohr Siebeck

Lessig, L. (2002), Privacy as Property, 69 Social Research 247
Luhmann, N. (2012), Macht, 4th ed., UTB
Marauhn, T. / Thorn, J. (2013), Kapitel 16: Privat- und Familienleben, in: O. Dörr / R. Grote / T. Marauhn (Eds.), EMRK/GG Konkordanzkommentar zum europäischen und deutschen Grundrechtsschutz, 2nd ed., Mohr Siebeck
Masing, J. (2012), Herausforderungen des Datenschutzes, 65 Neue Juristische Wochenschrift 2305
Mayer-Schönberger, V. / Padova, Y. (2016), Regime change? Enabling Big Data through Europe's new Data Protection Regulation, 17 The Columbia Science & Technology Review 315
Monopolkommission (2015), Sondergutachten 68 – Wettbewerbspolitik: Herausforderungen digitale Märkte, 1 June 2015, available at: www.monopolkommission.de/index.php/de/gutachten/sondergutachten/sondergutachten-68
Möslein, F. (2016), Private Macht, Mohr Siebeck
Müller, G. / Flender, C. / Peters, M. (2012), Vertrauensinfrastruktur und Privatheit als ökonomische Fragestellung, in: J. Buchmann (Ed.), Internet Privacy – eine multidisziplinäre Bestandsaufnahme, 143, acatech
Nissenbaum, H. (2010), Privacy in Context – Technology, Policy, and the Integrity in Social Life, Stanford Law Books
Pasquale, F. (2013), Privacy, Antitrust, and Power, 20 George Mason Law Review 1009
Picker, R. (2008), Competition and Privacy in Web 2.0 and the Cloud, 102 Northwestern University Law Review 1
Posner, R.A. (1981), The Economics of Privacy, 71 The American Economic Review 405
Pozzato, V. (2014), Opinion of the European Data Protection Supervisor: Interplay Between Data Protection and Competition Law, 4 Journal of European Competition Law & Practice 468
Purtova, N. (2010), Property in personal data: A European perspective on the instrumentalist theory of propertisation, 2 European Journal of Legal Studies 193
Purtova, N. (2011), Property Rights in Personal Data – A European Perspective, Wolters Kluwer
Purtova, N. (2015), The Illusion of Personal Data as No One's Property, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2346693
Renner, M. (2016), Machtbegriffe zwischen Privatrecht und Gesellschaftstheorie, in: F. Möslein (Ed.), Private Macht, 505, Mohr Siebeck
Rees, C. (2013), Tomorrow's privacy: personal information as property, 3 International Data Privacy Law 220
Richards, N. / King, J. (2014), Big Data Ethics, 49 Wake Forest Law Review 393
Riesenhuber, K. (2016), Private Macht im Vertragsrecht – Langzeitverträge, in: F. Möslein (Ed.), Private Macht, 193, Mohr Siebeck
Rölli, M. (2016), Vorüberlegungen zu einer Philosophie der privaten Macht – im Ausgang von einigen allgemeinen Bemerkungen zum philosophischen Stand der Machttheorie, in: F. Möslein (Ed.), Private Macht, 83, Mohr Siebeck
Rössler, B. (2001), Der Wert des Privaten, Suhrkamp
Roßnagel, A. / Richter, P. / Nebel, M. (2012), Internet Privacy aus rechtswissenschaftlicher Sicht, in: J. Buchmann (Ed.), Internet Privacy – eine multidisziplinäre Bestandsaufnahme, 281, acatech
Roth, W.-H. (2006), Zur Berücksichtigung nichtwettbewerblicher Ziele im europäischen Kartellrecht – eine Skizze –, in: C. Engel / W. Möschel (Eds.), Recht und spontane Ordnung: Festschrift für Ernst-Joachim Mestmäcker zum achtzigsten Geburtstag, 411, Nomos
Schaar, P. (2016), Algorithmentransparenz, in: A. Dix / G. Franßen / M. Kloepfer / P. Schaar / F. Schoch / A. Voßhoff (Eds.), Deutsche Gesellschaft für Informationsfreiheit, Informationsfreiheit und Informationsrecht – Jahrbuch 2015, 23, Lexxion
Schäfer, H.-B. / Ott, C. (2005), Lehrbuch der ökonomischen Analyse des Zivilrechts, 4th ed., Springer
Schantz, P. (2016), Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, 69 Neue Juristische Wochenschrift 1841
Schwartz, P.M. (2004), Property, Privacy and Personal Data, 118 Harvard Law Review 2055

Schwartmann, R. / Hentsch, C.-H. (2015), Eigentum an Daten – Das Urheberrecht als Pate für ein Datenverwertungsrecht, Recht der Datenverarbeitung, 221
Schwenke, C. (2005), Individualisierung und Datenschutz, Rechtskonformer Umgang mit personenbezogenen Daten im Kontext der Individualisierung, Deutscher Universitäts-Verlag
Schwenke, T. (2013), Nutzungsbedingungen sozialer Netzwerke und Onlineplattformen, 59 Wettbewerb in Recht und Praxis 37
Schweitzer, H. (2016), Wettbewerbsrecht und das Problem privater Macht, in: F. Möslein (Ed.), Private Macht, 447, Mohr Siebeck
Schweitzer, H. / Fetzer, T. / Peitz, M. (2016), Digitale Plattformen: Bausteine für einen künftigen Ordnungsrahmen, ZEW Discussion Paper No. 16-042, available at: www.jura.fu-belin.de/fachbereich/einrichtungen/zivilrecht/lehrende/schweitzerh/informationen/Schweitzer-Fetzer-Peitz-dp16042.pdf
Spiekermann, S. / Acquisti, A. / Böhme, R. / Hui, K.-L. (2015), The challenges of personal data markets and privacy, 25 Electronic Markets 161
Spindler, G. (2014), Datenschutz- und Persönlichkeitsrechte im Internet – Der Rahmen für Forschungsaufgaben und Reformbedarf, Beilage 116 GRUR 101
Spindler, G. (2016), Digitale Wirtschaft – analoges Recht: Braucht das BGB ein Update?, 71 Juristen Zeitung 805
Sofsky, W. (2007), Verteidigung des Privaten: Eine Streitschrift, C.H.Beck
Solove, D. (2001), Privacy and Power: Computer Databases and Metaphors for Information Privacy, 53 Stanford Law Review 1393
Solove, D. (2007), "I've Got Nothing to Hide" and Other Misunderstandings of Privacy, 44 San Diego Law Review 745
Swire, R. (2007), Protecting Consumers: Privacy Matters in Antitrust Analysis, Center for American Progress of 19 October 2007, available at: https://www.americanprogress.org/issues/economy/news/2007/10/19/3564/protecting-consumers-privacy-matters-in-antitrust-analysis/
Swire, P. / Lagos, Y. (2013), Why the right to data portability likely reduces consumer welfare: Antitrust and privacy critique, 73 Maryland Law Review 2335
Tan, S. (2007), Defining Social Algorithm, available at: http://ezinearticles.com/?Defining-Social-Algorithm&id=403407
Vanberg, V.J. (2011), Consumer welfare, total welfare and economic freedom – on the normative foundations of competition policy, in: J. Drexl / W. Kerber / R. Podszun (Eds.), Competition Policy and the Economic Approach, 44, Edward Elgar
van Loenen, B. / Kulk, S. / Ploeger, H. (2016), Data protection legislation: A very hungry caterpillar – The case of mapping data in the European Union, 33 Government Information Quarterly 338
von Lewinski, K. (2014), Die Matrix des Datenschutzes – Besichtigung und Ordnung eines Begriffsfeldes, Mohr Siebeck
von Walter, A. (2014), Datenschutz-Rechtsbruch als unlauteres Marktverhalten? Zum Verhältnis des Lauterkeitsrechts zum Datenschutzrecht, in: T. Lettl / J. Fritzsche / B. Buchner / C. Alexander (Eds.), Festschrift für Helmut Köhler zum 70. Geburtstag, 771, C.H. Beck
Warren, M. E. (1992), Max Weber's Nietzschean conception of power, 1992, History of the Human Sciences, 19, SAGE
Weatherill, S. (2013), EU Consumer Law and Policy, 2nd ed., Edward Elgar
Weber, M. (1972), Wirtschaft und Gesellschaft, 5th ed., Mohr Siebeck
Weichert, T. (2014), Scoring in Zeiten von Big Data, 47 Zeitschrift für Rechtspolitik 168
Wish, R. / Bailey, D. (2011), Competition Law, 7th ed., Oxford University Press
World Economic Forum (2014), Rethinking Personal Data: A New Lens for Strengthening Trust, available at: www3.weforum.org/docs/WEF_RethinkingPersonalData_ANewLens_Report_2014.pdf
Zimmer, D. (2011), Consumer welfare, economic freedom and the moral quality of competition law – comments on Gregory Werden and Victor Vanberg, in: J. Drexl / W. Kerber / R. Podszun (Eds.), Competition Policy and the Economic Approach, 72, Edward Elgar