TRADE SECRECY AND INTERNATIONAL TRANSACTIONS

LAW AND PRACTICE

ELIZABETH A. ROWE
SHARON K. SANDEEN

ELGAR INTELLECTUAL PROPERTY LAW AND PRACTICE

TRADE SECRECY AND INTERNATIONAL TRANSACTIONS

ELGAR INTELLECTUAL PROPERTY LAW AND PRACTICE

Series Editors: Trevor Cook, *Partner, Bird & Bird* and Johanna Gibson, *Herchel Smith Professor of Intellectual Property Law, Queen Mary University of London*

The Elgar Intellectual Property Law and Practice series is a library of works by leading practitioners and scholars covering discrete areas of law in the field of intellectual property. Each title will describe the law in detail, but will also be deeply analytical, highlighting and unpicking the legal issues that are most critical and relevant to practice. Designed to be detailed, focused reference works, the books in this series aim to offer an authoritative statement on the law and practice in key topics within the field, from *Trade Marks* to *Pharmaceuticals*, from *Patent Standards* to *Trade Secrecy* and from *IP Licensing* to *IP Valuation*.

Titles in this series include:

The Law and Regulation of Franchising in the EU
Mark Abell

The Protection of Geographical Indications
Michael Blakeney

Patent Law in Greater China
Edited by Stefan Luginbuehl and Peter Ganea

Trade Secrecy and International Transactions
Elizabeth A. Rowe and Sharon K. Sandeen

TRADE SECRECY AND INTERNATIONAL TRANSACTIONS

Law and Practice

ELIZABETH A. ROWE

Professor of Law, University of Florida, Levin College of Law, USA

SHARON K. SANDEEN

Professor of Law, Hamline University School of Law, USA

ELGAR INTELLECTUAL PROPERTY LAW AND PRACTICE

Edward Elgar PUBLISHING

Cheltenham, UK • Northampton, MA, USA

Published by
Edward Elgar Publishing Limited
The Lypiatts
15 Lansdown Road
Cheltenham
Glos GL50 2JA
UK

Edward Elgar Publishing, Inc.
William Pratt House
9 Dewey Court
Northampton
Massachusetts 01060
USA

A catalogue record for this book
is available from the British Library

Library of Congress Control Number: 2015935882

This book is available electronically in the Elgaronline
Law subject collection
DOI 10.4337/9781782540786

ISBN 978 1 78254 077 9 (cased)
ISBN 978 1 78254 078 6 (eBook)

Typeset by Columns Design XML Ltd, Reading
Printed and bound in Great Britain by T.J. International Ltd, Padstow

CONTENTS

EXTENDED TABLE OF CONTENTS

PREFACE

We are pleased to offer this book as a concise and authoritative source on trade secrecy in international transactions. It is intended as a starting point for research and as a handbook for understanding and approaching the laws pertaining to trade secrets and confidential (or undisclosed) information throughout the world. It is unique in that it provides a careful and balanced view that integrates a macro-level explanation of the international framework for protecting trade secrets and other proprietary information with a micro-level analysis of the trade secret laws of eight representative countries, including the United States.

Because the trade secret law of the United States is often promoted as the international standard for trade secret protection, this book provides a detailed explanation of the scope and limits of trade secret law in the United States. This explanation of the US system then serves as the basis to organize, compare and understand the parallel laws of Brazil, Canada, China, India, Japan, Mexico and the United Kingdom. It is also the first book to present an in-depth analysis of the European Union Directive on trade secret law that compares the proposed Directive (as amended by the EU Council) with the trade secret principles of the United States.

In a well-organized and easy to read manner, this book provides practical advice on how businesses can enhance trade secret protection and enforcement while engaging in global commerce. One of its valuable contributions is the presentation of a suggested process for learning, understanding and applying the trade secret laws of other countries, including information about the various legal systems of the world. It is filled with insights about international trade secret law, including observations about the increased attention being paid to trade secret principles by policy-makers on both sides of the Atlantic and the Pacific.

The general organization of the book follows a logical and analytical approach to understanding international trade secret law, organized into two parts. Part I begins with an introduction and road-map to understanding trade secret law and the importance of trade secrets to global commerce. It then follows with an explanation of the TRIPS Agreement and its relevance in setting basic standards for countries to protect undisclosed information. The book then introduces and explains the US approach to trade secrecy based upon the Uniform Trade Secrets Act. Topics covered include: (1) the scope of trade secret protection; (2) the requirements for establishing trade secret rights; (3) the legal and policy limitations of trade secret protection; (4) the essential elements of a claim for trade secret misappropriation; (5) major defences; and (6) available remedies. Part I ends with another unique feature of this book. It addresses the challenges of protecting trade secrets in dealings with the government and discusses data exclusivity issues related to the required submission of information to government

officials as part of a regulatory process. The data exclusivity issues often, but not always, interrelate with trade secrecy concerns as well as government transparency and free competition interests.

In Part II of the book, the general framework and areas discussed under US law are then applied individually to seven countries. Part II first discusses the basic features of both common law and civil law systems and then discusses the specific legal traditions and trade secret principles of three common law countries and four civil law countries. The discussion for each of the featured countries is organized around the key issues of most relevance to practitioners. These include: (1) an overview of the country's legal system, including whether or not it is a civil or common law country; (2) the contours of its trade secret law; (3) principles governing trade secrecy in employment relationships; (4) principles governing trade secrecy in business relationships; (5) the criminal consequences for trade secret misappropriation; and (6) general information concerning the rules and practice for litigating trade secret disputes. Appendix 1 to the book is an analysis of the proposed EU Trade Secret Directive as compared to US law. Appendix 2 is a reprint of the EU Trade Secret Directive as originally proposed in November 2013, with EU Council amendments from May 2014 interposed therein. Thus, it is a handy and useful reference for determining both the details of the Directive and the issues that were of concern to the EU Council. Both Appendices can also be used to compare and contrast the proposed EU Directive to the laws of non-EU countries.

We hope that this book will serve as a valuable resource concerning the questions and issues that arise about trade secrecy while doing business across borders and as a guide for policy-makers who are seeking to amend the trade secret laws of their country. At a minimum, it will help attorneys throughout the world to understand basic trade secret principles and to assist their clients to institute the 'reasonable efforts' that are typically necessary to protect trade secrets.

Elizabeth A. Rowe
Sharon K. Sandeen

ACKNOWLEDGEMENTS

We would like to extend our gratitude to the many people who have assisted us in the preparation and publication of this book, including attorneys and scholars in various countries who provided valuable insights or reviews of the materials pertaining to their country's laws. We specifically acknowledge: Ken Port and Christoph Rademacher for their reviews of the section on Japan; Laura Wen-yu Young for her review and contributions to the section on China; Christina Guerra for her review of the section on Brazil; David Flint and Sonja Hart for their contributions to the section on the United Kingdom; and Lisa R. Lifshitz for her review of the section on Canada.

Professor Rowe wishes to acknowledge her research assistants Garrett Tozier, Matthew Morrow and Eric Van Wiltenburg for their excellent work on this project. She would also like to thank her husband and children for their support.

Professor Sandeen wishes to thank her research assistants Julianna Passe, Colin Thomsen and Frances Yanke, as well as the library staff of Hamline University School of Law and all of her other research assistants who have helped her with trade secret research over the years.

Finally, we gratefully acknowledge Edward Elgar Publishing and its editors for recognizing the value of this kind of resource to an international audience and bringing it to market.

ABBREVIATIONS

AIC	Administration for Industry and Commerce (China)
ALJ	Administrative Law Judge
BPTO	Brazilian Patent and Trademark Office
BRIC	Brazil, Russia, India and China
CCP	Code of Civil Procedure (Japan)
CFAA	Computer Fraud and Abuse Act (US)
CIETAC	China International Economic and Trade Arbitration Commission
CPR	Civil Procedure Rules (UK)
EEA	Economic Espionage Act (US)
EFTA	European Free Trade Association
EM	Explanatory Memorandum to Proposed EU Trade Secret Directive
FCC	Federal Civil Code (Mexico)
FDA	Food and Drug Administration (US)
FLL	Federal Labour Law (Mexico)
FPC	Federal Penal Code (Mexico)
FTA	Free Trade Agreement
FTC	Federal Trade Commission (US)
IP	intellectual property
IPL	Industrial Property Law (Brazil and Mexico)
IPR	intellectual property right
ITC	International Trade Commission (US)
JFTC	Fair Trade Commission (Japan)
METI	Ministry of Economy, Trade and Industry (Japan)
NAFTA	North American Free Trade Agreement
NDA	non-disclosure agreement
NME	new molecular entity
NPC	National People's Congress (China)
OECD	Organisation for Economic Co-operation and Development
PI	preliminary injunction
R&D	research and development
SAIC	State Administration for Industry and Commerce (China)
SEC	Securities and Exchange Commission (US)
SIA	Security of Information Act (Canada)
TFEU	Treaty on the Functioning of the European Union
TPPA	Trans-Pacific Partnership Agreement
TRIPS	Agreement on Trade-Related Aspects of Intellectual Property Rights
TRO	temporary restraining order
TSPI	Trade Secret Protection Index
TTIP	Trans-Atlantic Trade and Investment Partnership

UCL	Unfair Competition Law (China)
UCPL	Unfair Competition Prevention Law (Japan)
USTR	United States Trade Representative
UTSA	Uniform Trade Secrets Act (US)
WIPO	World Intellectual Property Organization
WTO	World Trade Organization

TABLE OF CASES

Japan

United Kingdom

United States of America

TABLE OF LEGISLATION

India

Japan

Mexico

Taiwan

United Kingdom

United States of America

International

Free Trade Agreements

Part I

TRIPS REQUIREMENTS AND THE FUNDAMENTALS OF US TRADE SECRET LAW

1

INTRODUCTION

I. ABOUT THIS BOOK

1.01 Ask any business, large or small, to identify one of its most important assets and it is bound to identify its confidential and proprietary information or 'trade secrets'. This is because it is in the nature of businesses to try to secure a competitive advantage over rivals and inventing the proverbial 'better mouse-trap' is one way to do so. Frequently, businesses that invent or create something new will seek patent protection for their inventions or rely upon copyright protection for their creations and writings. However, for a number of reasons (including the costs of patent prosecution and enforcement) they often choose to rely on secrecy instead. Even if they choose to patent their inventions there is a period of time during the research and development process and before any patent application is published where secrecy is important and where the laws governing the protection of business information are of great significance.

1.02 This book explains the scope and limits of the law governing the protection of business secrets and provides practical advice on how to protect those secrets while still engaging in global commerce. It begins in Part I with a detailed examination of the meaning and application of trade secret law in the United States. Part II then provides information concerning the process for learning and understanding the laws of other countries and follows with overviews of the trade secret laws of seven countries: Brazil, Canada, China, India, Mexico, Japan and the United Kingdom.

1.03 Part I begins with this introductory chapter by providing some background concerning the history, purpose and limits of trade secrecy. It then provides observations about the increased attention being paid to trade secrets by

policy-makers on both sides of the Atlantic and the Pacific, and preliminary information about the international norm-making process with respect to trade secrets.

1.04 Because the current international norms concerning trade secret protection are expressed in an Annex to the agreement which established the World Trade Organization (WTO), known as the Agreement on Trade-Related Aspects of Intellectual Property Law and often referred to as the TRIPS Agreement,[1] Chapter 2 examines the history, purpose and scope of Article 39 of the TRIPS Agreement.[2] As is explained therein, although there was great reluctance (particularly in the developing world) to recognize trade secrets as an intellectual property right (IPR) and include trade secret protection requirements in the TRIPS Agreement, ultimately the United States and its allies succeeded in their efforts to include some trade secret (labelled 'undisclosed information') provisions in the TRIPS Agreement. Specifically, Articles 39.1 and 39.2 were included to recognize trade secret misappropriation as a form of unfair business practice and to define trade secrets and the act of misappropriation in accordance with the predominant trade secret law of the United States, the Uniform Trade Secrets Act (UTSA).[3]

1.05 Chapter 3 discusses the history, scope and limits of the UTSA, including the three requirements for trade secrecy and the meaning of misappropriation as reflected in Article 39.2 of the TRIPS Agreement. Because current international trade secrecy norms and harmonization efforts are based principally on the UTSA, and the UTSA is the model for increased trade secret protection in the European Union (EU), it provides an important baseline for understanding trade secret laws from around the world. In Part II of this book, the various provisions of the UTSA (and US trade secret principles more generally) are used to compare and contrast the laws of other countries.

1.06 By understanding the details and limits of the UTSA, attorneys who are retained to assist their clients to protect trade secrets in any given country will, at the very least, be equipped with sufficient knowledge to ask questions about the particulars of that country's trade secret laws. In countries that have adopted UTSA-style laws (like the proposed EU Trade Secret Directive and the laws of

1 Agreement on Trade-Related Aspects of Intellectual Property Rights, 15 April 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, The Legal Texts: The Results of the Uruguay Round of Multilateral Trade Negotiations (1999), p. 320, 1869 UNTS 299, (1994) 33 ILM 1197 ('TRIPS Agreement').

2 See also, Sharon K. Sandeen, 'The Limits of Trade Secret Law: Article 39 of the TRIPS Agreement and the Uniform Trade Secrets Act on Which It is Based' in Rochelle C. Dreyfuss and Katherine J. Strandburg (eds), *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research* (2011), p. 537.

3 See UTSA (1985), s. 1(4), for the definition of 'trade secret'; see also UTSA, s. 1(2), for the definition of 'misappropriation'.

Japan and Taiwan), the interpretation and application of the UTSA in the United States may have more direct application, at least as secondary authority.

1.07 Importantly, while the UTSA is primarily designed to help information owners protect information that qualifies for trade secret protection, US trade secret law as expressed in the UTSA and related case law seeks (like most IP laws) to achieve an appropriate balance between trade secret protection and principles of free competition. Because of this, it is important to understand that trade secret law does not protect all business information (or even all secret business information), but only a specific subset of that information. This is because, from a societal point of view, the dissemination of information and knowledge is viewed as important for both human and economic development. Related to this is the concern that if trade secret protection is too strong it will dissuade inventors from seeking patent protection where disclosure is an explicit part of the trade-off.

1.08 From a business point of view, the limited scope of trade secret protection means that trade secret law cannot be relied upon to protect all important business information and that other strategies (principally, technical and contractual) should be utilized as necessary. In other words, self-help measures are often more effective than reliance upon trade secret law and enforcement. However, as explained in Chapter 4, businesses should always balance the costs and benefits of self-help, including not only the costs of required security measures but the potential costs associated with restrictions on information flows and employee mobility.

1.09 As many trade secret owners know, there is more to protecting trade secrets than knowing the applicable law. As a practical matter, no company ever wants to be in a position of having to seek enforcement of its trade secret rights because, when they do, chances are that their trade secrets have already been compromised. Thus, an important part of representing clients in trade secret matters involves early planning and intervention and frequent monitoring of trade secret usage. Chapters 4 and 5 of this book address these subjects by explaining strategies and best practices for protecting trade secrets and other business information in two contexts: (1) externally with respect to off-site relationships with non-employees such as vendor and independent contractor relationships; and (2) internally with respect to employees and the on-site agents of a company.

1.10 Chapter 6 provides a detailed examination of the available procedures for enforcing trade secret rights under US law as a prelude to the country overviews that follow in Part II. Since the WTO Agreement was entered into more than

20 years ago, the enforcement of its provisions and the enforcement of the legal protections that it requires each of its members to provide has been a major focus of attention, particularly with respect to the asserted lack of enforcement of IPRs. Thus, it is no surprise that recent efforts to harmonize trade secret laws focus on issues related to the enforcement of trade secret rights. Consistent with recent harmonization efforts, Chapter 6 discusses available civil actions, criminal prosecution and cross-border measures. It also provides practical tips that should be followed to enhance the effective enforcement of trade secret rights.

1.11 Chapter 7 addresses a special issue known as 'data exclusivity' that sometimes involves trade secrets but, more broadly, concerns the required submission of information to governmental officials as part of a regulatory process. Data exclusivity is the topic of Article 39.3 of the TRIPS Agreement and is the subject of increased calls to limit what the 2014 Special 301 Report by the US Trade Representative has labelled 'forced technology transfer'.[4] Although data exclusivity does not concern trade secrets exclusively (and sometimes not at all), it is important to understand that calls for increased data exclusivity by various regulated industries are often coupled with calls for greater trade secret protection. It is also important to consider how data exclusivity laws relate to the principles of government transparency and free competition and whether they are a good idea in all contexts.

1.12 Although it is not possible in this book to provide a survey of all of the trade secret laws for every country, Part II provides information about the trade secret laws of many of the most important trading partners of the United States and EU countries organized around the key issues that are identified in Chapters 1 through 6. It begins with Chapter 8 which provides general information about the various legal systems of the world (principally the common law and civil law systems) that can be applied to countries that are not discussed directly. As is explained, understanding the legal structure and sources of law of other countries is critical both to finding the trade secret principles of other countries and to knowing how those principles are likely to be applied.

1.13 The remaining chapters of the book examine the laws of seven countries grouped in accordance with their applicable legal traditions. Chapter 9 discusses the specific laws of three common law countries: the United Kingdom, Canada and India. Chapter 10 discusses the laws of four civil law countries: Brazil, China, Japan and Mexico.

4 Office of the US Trade Representative, *2014 Special 301 Report* (2014), available at www.ustr.gov/sites/default/files/USTR%202014%20Special%20301%20Report%20to%20Congress%20FINAL.pdf.

1.14 The book ends with two Appendices that focus on the proposed EU Directive 'on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure' ('EU Trade Secret Directive').[5] When adopted, it will require all EU member countries to amend their laws as necessary to provide greater and more harmonized protection for trade secrets.

1.15 Appendix 1 provides an analysis of the proposed Directive that details the similarities and differences between the Directive and US trade secret law and highlights some of its ambiguities. It is followed in Appendix 2 by a redlined version of the proposed Directive showing how the original proposal was amended by the EU Council. This document is helpful for illustrating the issues that were of concern to EU member countries as well as possible points of divergence as other countries move to improve their trade secret laws.

1.16 As will be seen, although the proposed Directive is obviously modelled after the UTSA, as proposed, it includes some provisions that are not an express part of the UTSA but which, in many cases, are consistent with the common law application of the UTSA within the United States. However, an important feature of the proposed EU Trade Secret Directive that is not an explicit part of the UTSA concerns various public interest exceptions to trade secret misappropriation claims.

1.17 The text of the trade secret laws that have been adopted by various countries mentioned in this book are not included in the Appendices due to space considerations, however, they are usually available online in their native language as well as in other languages. As further explained below, both the WTO website and the website of the World Intellectual Property Organization (WIPO) are good resources for information concerning such legal texts, although care must be taken to determine if the information is up to date. This is particularly true with respect to civil law countries where laws evolve through frequent formal amendments.

5 European Commission, *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*, 2013/0402 (COD) (2013), reprinted as amended in Appendix 2 and available at http://eur-lex.europa.eu/legal-content/EN/ALL/;ELX_SESSIONID=0ylTTfHT0xDTvYWCPhmQXCLQNJcygP6zJlyLLNxnGvdN9b40YFyy!-1932605564?uri=CELEX:52013PC0813.

II. A ROAD-MAP FOR UNDERSTANDING TRADE SECRET LAW

1.18 International trade secret law is currently a moving target, particularly outside of the United States. Although the basic requirements for protection and the basic definitions of a trade secret and of misappropriation were established by the TRIPS Agreement, as the drafting history of the UTSA and a study by the European Commission demonstrate, more details and harmonization are believed necessary to ensure greater predictability and balance in trade secret cases.[6] However, it remains to be seen how the trade secret laws of each country are drawn and applied, particularly in light of the fact that several ancillary areas of law often dictate outcomes in trade secret cases.

1.19 Fortunately, the issues that were addressed more than 35 years ago by the drafters of the UTSA, and more recently in the European Commission Study, provide a road-map for attorneys to use when considering the trade secret laws of countries that have not yet adopted UTSA-style laws. These issues include:

(1) the definition of a trade secret;
(2) the definition of misappropriation, including whether it prohibits wrongful acquisition of trade secrets as well as wrongful disclosure or use of trade secrets;
(3) the definition of proper means to acquire trade secrets;
(4) the availability of remedies, including the applicable measure of damages;
(5) the availability of timely preliminary relief;
(6) the liability of third parties (typically, those not in privity with the trade secret owner) who come to possess trade secrets;
(7) the availability of protective orders to protect trade secrets during and after the pendency of litigation;
(8) the availability, nature and scope of means to enforce trade secret rights, including civil, criminal and cross-border measures; and
(9) the interrelationship between trade secrecy and principles regarding competition, the diffusion of knowledge and employee mobility.

The chapters that follow, particularly Chapters 3, 6, 8, 9 and 10, provide information to help all attorneys and counsellors understand the significance of the foregoing issues and how UTSA-styled trade secret laws seek to achieve the

6 For the drafting history of the UTSA, see Sharon K. Sandeen, 'The Evolution of Trade Secret Law and Why Courts Commit Error When They Do Not Follow the Uniform Trade Secrets Act' (2010) 33 *Hamline L Rev.* 493, reproduced in Sharon K. Sandeen and Elizabeth A. Rowe (eds), *Trade Secrets and Undisclosed Information* (2014). See also, European Commission, *Study on Trade Secrets and Confidential Business Information in the Internal Market*, ('European Commission Study'), available at http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_final-study_en.pdf.

proper balance between protecting legitimate trade secrets and ensuring the proper conditions for free competition, the diffusion of knowledge and employee mobility.

1.20 As discussed in Chapters 4 and 5, in applying trade secret law in a given country it is also important to consider whether any special rules or other legal principles apply to the employment relationship and to business-to-business relationships. Questions to consider in this regard include:

(1) Does the country view trade secrets as a form of property (with exclusive rights similar to patent and copyright law) or is trade secret misappropriation a form of unfair competition?
(2) Who owns trade secrets created by employees and how is ownership obtained and transferred?
(3) What are the country's views with respect to employee mobility, including the enforceability of non-compete agreements, invention assignment agreements and confidentiality agreements?
(4) Can a duty to protect trade secrets be implied or must it be established in a written document or other express contract? In other words, how are obligations of confidentiality formed? Is a written contract required?
(5) Must technology licensing agreements be reviewed and approved by governmental officials?

1.21 Finally, as further discussed in Chapter 8, in addition to considering the specific laws and legal principles that may govern the protection of trade secrets in a given country, consideration must also be given to the history, culture, legal system, procedures and traditions of each country. This is particularly true with respect to available remedies and their enforcement and the process of negotiating contracts concerning the licensing and protection of trade secret rights.

III. THEORY, PURPOSE AND LIMITS OF TRADE SECRET LAW

1.22 Based upon the rhetoric contained in various position papers and statements of both the United States and the EU, increased trade secret protection is touted as an essential component of innovation, the principal argument being that it is needed to spur innovation and creativity (the incentive rationale of trade secrecy).[7] At the same time, it is recognized that the over-protection of information and the over-assertion of trade secret rights can adversely affect

7 See e.g., European Commission Study, n. 6 above.

employee mobility, the diffusion of knowledge and otherwise have anticompetitive consequences.[8] Thus, few policy-makers advocate for the absolute protection of business information (or even trade secrets) and, accordingly, numerous limiting doctrines exist under US trade secret law and the proposed EU Trade Secret Directive that are specifically designed to ensure that trade secret protection is weaker than patent protection. This is because patent law is designed to provide the primary incentive for invention and includes an important disclosure requirement.

1.23 Despite the importance of patent law in incentivizing invention, it has been recognized by the US Supreme Court that there is nothing inherently wrong with a system of legal protection that complements patent protection.[9] Thus, it is generally recognized that the incentive rationale also applies to trade secret protection. However, conflicts between trade secret protection and the patent policy of disclosure (as well as the copyright policy of disclosure) can develop when trade secret law (or any other law) is seen as a more viable alternative to patent protection, at least with respect to patentable inventions or so-called 'technical trade secrets'.[10] This explains, in part, the limits that are typically placed upon the scope of trade secret rights.

1.24 The limits that are placed upon trade secret rights are also explained by the value that free market economies typically place on the dissemination of knowledge and employee mobility.[11] The importance of the dissemination of knowledge is why so many public funds are spent on public education, publicly funded research and public libraries, and why the developing world clamours for more education and technology transfer. However, unlike patented inventions which must be disclosed, trade secrets are not the type of information from which others can readily learn or upon which they can build, unless the information leaks out or is voluntarily shared. Thus, as explained by the US Supreme Court in *Kewanee* v. *Bicron Oil Co.*, the limits that are placed on trade secret protection in the United States are designed to ensure that a core of information (and the knowledge it conveys) remains free for everyone to use.[12]

---

8 Michael Risch, 'Trade Secret Law and Information Development Incentives' in Rochelle C. Dreyfuss and Katherine J. Strandburg (eds), *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research* (2011), p. 152; Orly Lobel, *Talent Wants to be Free: Why We Should Learn to Love Leaks, Raids and Free Riding* (2013).

9 *Kewanee Oil Co.* v. *Bicron Corp.*, 416 US 470 (1974).

10 A distinction is made in the law and literature between technical trade secrets and other trade secrets. Technical trade secrets concern information that is within patentable subject, traditionally defined not to include business methods. Non-technical trade secrets refer to everything else, including compilation of information and improved methods of organizing and conducting businesses. This distinction is important to keep in mind since some countries and courts are more comfortable protecting technical trade secrets.

11 Lobel, n. 8 above.

12 *Kewanee Oil Co.*, n. 9 above.

Under well-established trade secret doctrine in the United States (and as detailed in the EU Trade Secret Directive, see Appendix 2), this includes: (1) the general knowledge and skill that is acquired by learned and experienced individuals; (2) information that is generally known by the public and among people who are skilled in a particular art; and (3) information that is readily ascertainable.

1.25 While the incentive rationale of trade secret protection is most often cited by policy-makers, in reality there is nothing that prevents an inventor or creator from innovating in secret within the confines of her own home or place of business. In fact, this sort of innovation happens all the time and is sure to continue with or without trade secret protection. Moreover, when the business activities of a given country are largely localized and consist of small groups of people (often family members) working together, there is not as much risk that 'secret' information will be shared with outsiders, let alone misappropriated. As an economy moves toward larger-scale enterprises and increases its foreign investment and trade, however, the dynamics change. Trade secret issues generally arise when the person who invented or created the secret information wants to share it with another either because it must be shared and used to have value or because the inventor wants to obtain financing or sell the invention.

1.26 The necessary sharing of business information as economies and industries grow and develop places trade secrets at greater risk of loss and has been used as the basis for two additional justifications for trade secret protection. First, the US Supreme Court and others have noted that trade secret law promotes the sharing of information by making it possible for trade secret owners to disclose their trade secrets in limited circumstances without suffering a loss of trade secrets rights (the disclosure purpose of trade secret law).[13] Although this is not a degree of sharing that is similar to the *quid pro quo* of patent law (which explicitly makes public disclosure of the invention a condition of the grant of patent rights), the concern is that without trade secret protection, trade secret owners will be less willing to share information and the efficiencies and general knowledge transfer that could be achieved through limited sharing of valuable information would be lost.

1.27 Second, it is argued that without trade secret laws to protect information that is shared within a confidential relationship, trade secret owners would be inclined to spend too many resources to protect their secrets, including the increased

13 *Ibid.*; Sharon K. Sandeen, 'Kewanee Revisited: Returning to First Principles of Intellectual Property Law to Determine the Issue of Federal Preemption' (2008) 12 *Marq. Intell. Prop. L Rev.* 299; Mark A. Lemley, 'The Surprising Virtues of Treating Trade Secrets as IP Rights' in Rochelle C. Dreyfuss and Katherine J. Strandburg (eds), *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research* (2011), p. 109.

transaction costs associated with negotiated confidentiality agreements. This is the efficiency (or lowering of transaction costs) purpose of trade secret law.[14]

1.28 In part, the pressure to increase trade secret protection internationally is simply an extension of the classic justifications for trade secret protection, which historically focused on the maintenance of business ethics. But those companies that wish to protect their trade secrets (particularly in countries like the United States that already have well-developed trade secret principles) can already do so by confining the use and sharing of their trade secrets to countries where trade secret protection is strong. Seen in this light, recent efforts to increase trade secret protection internationally represent an obvious effort to broaden the geographic scope of the safe (or relatively so) sharing of information. In theory, this should be good for both economic development and technology transfer by allowing for the greater diffusion of knowledge, albeit with restrictions.

1.29 As expressed in the European Commission Study:

> The results of our exercise support the working hypothesis that new harmonized legislation directed at trade secrets would have a significant impact fostering innovation and economic growth, by removing currently existing obstacles to the smooth functioning of the Internal Market for know-how such as the high transaction costs and the higher risk associated with an inadequate legal framework throughout the Union.[15]

The problem with the goal of lowering transactions costs, however, is that despite the possibility that a harmonized trade secret law in the EU might make it easier for a trade secret owner to successfully assert a trade secret misappropriation claim, as discussed in Chapters 4 and 5, it is still highly recommended that trade secret owners enter into written agreements with every person and company who will be allowed to access their trade secrets.

1.30 Additionally, while the foregoing quote may explain the benefits of trade secret protection within common markets like the United States and the EU, the pressure to increase trade secret protection elsewhere (e.g., China, Brazil and India) is explained by a number of other factors, including the fear that some foreign countries have adopted the misappropriation of trade secrets and other business information as a central tenet of their innovation strategy, or worse, as a means to acquire sensitive information related to national security. There is also the 'if you build, they will come' argument (also made during the negotiations

14 Risch, n. 8 above.

15 European Commission Study, n. 6 above.

which led to the TRIPS Agreement) that posits: if developing countries create and maintain a robust and effective system of IPR protection, foreign investment and trade will follow.

1.31 Increased interest in the protection of trade secrets may also reflect the desire of product manufacturers to move existing domestic manufacturing processes to foreign countries. Or it may reflect a desire by manufacturing companies, particularly those that use and can maintain hidden processes, to shift their focus from patent protection to trade secret protection. For those companies that already utilize offshore manufacturing facilities, enhanced international trade secret protection is designed to improve the enforcement of trade secret rights and stem the alleged misappropriation of trade secrets by foreign countries or by trading partners that are located abroad. As suggested in both the European Commission Study and the USTR's 2014 Special 301 Report, efforts to increase trade secret protection also reflect the cross-border nature of modern manufacturing processes, with different pieces of products being made in different countries for assembly elsewhere.[16]

1.32 Whether the ability of companies to 'offshore' their manufacturing processes is a good idea depends upon the lens through which one looks. From the perspective of US manufacturing workers, it probably looks like a bad idea because the risk of loss of trade secrets is a factor that often motivates US companies to maintain domestic manufacturing facilities. However, from the point of view of manufacturers and consumers, there is the promise of greater corporate profits and lower consumer costs if manufacturing processes can be confidently sent to less expensive foreign facilities. Additionally, enhanced trade secret protection internationally should reduce the incidence of espionage by foreign interests, including state-sponsored actions and the actions of organized crime, provided that the adoption and enforcement of trade secret laws extends to such activities.

1.33 From the perspective of developing countries, increased trade secret protection should enhance the ability of local individuals and companies to protect their trade secrets and (in theory) will lead to more knowledge and technology transfer in the form of the sharing and leakage of trade secret information from outsiders. In this regard, Article 7 of the TRIPS Agreement sets forth one of the central tenets of that agreement when it states:

16 European Commission Study, n. 6 above, at 149; Office of the US Trade Representative, *2014 Special 301 Report*, n. 4 above, at 18.

> The protection and enforcement of intellectual property rights should contribute to the promotion of technological innovation and to the transfer and dissemination of technology, to the mutual advantage of producers and users of technological knowledge and in a manner conducive to social and economic welfare, and to a balance of rights and obligations.

Whether these laudable goals come to fruition ultimately depends upon the extent and application of trade secret protection, including applicable limiting doctrines, and whether Article 7 of the TRIPS Agreement will be interpreted as an outer constraint on the scope of trade secret protection.

1.34 As is detailed in Chapter 3, the limiting doctrines of trade secret law play a key role in ensuring that trade secrets are neither over-protected nor under-protected. In *Kewanee* v. *Bicron Oil Co.*, the US Supreme Court recognized that the necessary balance is generally achieved by recognizing that trade secret protection is like a 'sieve' for information; it does not provide absolute protection and the leakage of such information is generally good for society because it adds to the store of publicly available information.[17] Moreover, as noted previously, if trade secret protection is too strong, it may discourage inventors from applying for patents and, thereby, prevent the public disclosure of important knowledge upon which others can build in the future.

1.35 The limiting doctrines of trade secret law can take many forms and can be expressed in: (1) the explicit language of applicable codes; (2) in case decisions; or (3) in ancillary bodies of law such as antitrust or competition law and employment law. For instance, under the UTSA, important limiting principles are reflected in the definition of a trade secret, the recognized 'proper' means to acquire trade secrets and the limits that are placed on available remedies, particularly injunctive relief. As detailed in Appendix 1, the proposed EU Trade Secret Directive contains these same limitations and then some. Additionally, under US law and the laws of many other countries, general principles of unfair competition, the importance of the public domain, principles of free speech and principles governing employee mobility often apply to limit the effective scope of trade secret protection.

17 *Kewanee Oil Co.*, n. 9 above, at 490.

IV. THE INTERNATIONAL COMMUNITY AWAKENS TO THE IMPORTANCE OF TRADE SECRETS

1.36 After decades of being ignored (or relatively so),[18] trade secret rights have become a hot topic among international trade professionals and businesses alike. A primary driver of the increased attention is concern about foreign and cyber-espionage and the ease with which all manner of information that is stored and transmitted in digital form can be accessed and copied.

1.37 Although it is largely hidden from public view, cyber security professionals have reported that companies located within the United States and other industrialized countries are under a constant barrage of cyber-attacks from nuisance, organized crime and state-sponsored interests.[19] Thus, it is asserted that companies need more tools to combat such attacks and the institution of more effective trade secret laws is seen as one possible solution.

1.38 Partly in response to the threat of cyber-attacks, in February 2013, the Executive Office of the President of the United States issued the *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets*, promising to 'coordinate and improve' efforts to protect US innovation, including trade secrets.[20] Since that time, there has been a noticeable increase in the rhetoric of trade secret enforcement emanating from the Office of the United States Trade Representative (USTR), including the inclusion of trade secret concerns in the annual Special 301 Report. Among other statements, the 2014 Special 301 Report 'urges [United States'] trading partners to ensure that they have robust systems for protecting and enforcing trade secrets, including the availability of deterrent criminal penalties for trade secret theft'.[21] The 2014 Special 301 Report also cites with favour the proposed EU Trade Secret Directive to better harmonize trade secret protection principles in EU member countries.

---

18 See Sharon K. Sandeen, 'Trade Secret Law: The Cinderella of Intellectual Property Law' in Peter K. Yu (ed.), *Intellectual Property and Information Wealth: Issues and Practices in the Digital Age* (2007), p. i.

19 See e.g., Mandiant Intelligence Center Report, *APT1: Exposing One of China's Cyber Espionage Units* (19 February 2013).

20 Executive Office of the President of the United States, *Administration Strategy on Mitigating the Theft of US Trade Secrets* (2013), available at www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf.

21 Office of the US Trade Representative, *2014 Special 301 Report*, n. 4 above, at 16. See also, Victoria Espinel, *Launch of the Administration's Strategy to Mitigate the Theft of US Trade Secrets* (20 February 2013), available at www.whitehouse.gov/blog/2013/02/19/launch-administration-s-strategy-mitigate-theft-us-trade-secrets.

1.39 In April 2013, the European Commission issued a *Study on Trade Secrets and Confidential Business Information in the Internal Market* ('European Commission Study').[22] This led to the 28 November 2013 introduction of the proposed EU Trade Secret Directive.[23] Various countries in Asia have also given increased attention to trade secret protection in recent years. For instance, Japan (discussed below) has amended its trade secret laws several times over the past five years in ways that significantly improve trade secret protection.[24] In 2013, Taiwan adopted its Trade Secret Act with provisions that are very similar to the US model.[25]

1.40 The increased attention on trade secrecy in Europe coincides with the European Commission's adoption in May 2011 of its Europe 2020 strategy which calls for the creation of an 'Innovation Union', a subsequent EU conference entitled 'Trade Secrets: Supporting Innovation, Protecting Know-how' that took place on 29 June 2012 and later public consultations.[26] As the proposed EU Trade Secret Directive explains: '[T]he Commission has undertaken to create an Innovation Union, protecting investments in the knowledge base, reducing costly fragmentation, and making Europe a more rewarding place for innovation'.[27] It also follows the 2011 *Report on Trade Secrets for the European Commission* which provides a country by country summary of trade secret laws in EU countries and which criticized the lack of harmonization.[28]

1.41 In the United States, the increased attention on trade secret law coincides with the passage of the America Invents Act (which arguably increases the importance of trade secrecy for some industries), the 2012 publication by Create.org of a *White Paper on Trade Secret Theft*[29] and the 2012 publication of a book on economic development which discusses the importance of trade secret protection for innovation.[30] The increased attention also reflects the importance of trade secrets to businesses large and small and represents the next step in the evolution of international trade secrecy norms.

---

22 European Commission Study, n. 6 above.

23 European Commission, *Proposal for a Directive*, n. 5 above.

24 See discussion of Japanese trade secret law in Chapter 7.

25 Trade Secrets Act (Taiwan), effective 1 February 2013.

26 See European Union, *Europe 2020*, available at http://ec.europa.eu/europe2020/index_en.htm.

27 European Commission, *Proposal for a Directive*, n. 5 above, at 2.

28 See Hogans Lovells Int'l, LLP, *Report on Trade Secrets for the European Commission: Study on Trade Secrets and Parasitic Copying (Look-alikes),* MARKT/2010/20/D (23 September 2011), available at http://ec.europa.eu/internal_market/iprenforcement/docs/parasitic/201201-study_en.pdf.

29 Create.org is a non-profit advocacy group funded in part by Microsoft with the mission of 'promoting responsible business practices including respect for intellectual property'.

30 Robert D. Cooter and Hans-Bernd Schäfer, *Solomon's Knot: How Law Can End the Poverty of Nations* (2012).

1.42 What is different about recent efforts to increase the protection of trade secrecy internationally compared to previous efforts, particularly in the EU, is the expressed desire for more uniformity, specificity and harmonization with respect to the details and limits of trade secret law. This follows efforts, albeit from several decades earlier, to harmonize trade secret law among the various states of the United States that began with the adoption of the Uniform Trade Secrets Act in 1979.

1.43 Efforts to harmonize trade secret law outside of the United States and EU are also underway, most notably with respect to the United States' Free Trade Agreement (FTA) strategy which typically results in the ratcheting-up of required IPR protection for signatories to the Agreement. The most recent case in point is the Trans-Pacific Partnership Agreement (TPPA) which is currently being negotiated and which includes draft provisions that would require enhanced trade secret protection efforts by signatory countries.[31]

V. INTRODUCTION TO INTERNATIONAL NORM-MAKING

1.44 Well established principles of international law recognize that each country is a sovereign nation that is free to establish its own laws and legal systems as dictated by its own needs and values. Nonetheless, various diplomatic strategies and processes have been used over the centuries to require willing countries to meet specified minimum standards with respect to various legal issues. In the field of IPRs, there is a long-standing and rich history of multilateral agreements for the protection of IPRs, including the Paris Convention for the Protection of Industrial Property of 1883 ('Paris Convention')[32] and the Berne Convention for the Protection of Literary and Artistic Works of 1886 ('Berne Convention').[33] However, until the adoption of the TRIPS Agreement in 1994, no multilateral agreement for the protection of IPRs specifically addressed the issue of trade secret protection.

1.45 As is explained in greater detail in Chapter 2, interest in international norm-making with respect to trade secrets first began in the late 1980s in conjunction with the negotiations that resulted in the formation of the WTO and approval of the TRIPS Agreement. Before then, each country was free to

31 United States Trade Representative *et al.*, Trans-Pacific Partnership Agreement (TTP) (2013), available at www.eff.org/issues/tpp.

32 Paris Convention for the Protection of Industrial Property, 20 March 1883, 21 UST 1583, 828 UNTS 305 (as amended on 28 September 1979).

33 Berne Convention for the Protection of Literary and Artistic Works, 9 September 1886, 25 UST 1341, 828 UNTS 221 (as amended on 28 September 1979).

develop its own legal principles with respect to the protection of proprietary information and, as one might expect, the scope and nature of those laws varied as a result. This is particularly true when one considers that the development of trade secret principles in England and the United States grew out of changes in the structure and purpose of companies during the first and second Industrial Revolutions and that not all countries enjoyed similar industrial development at the same time, or ever.[34]

1.46 Generally, as the economies of countries develop so that the sharing of information among businesses is more common and necessary, and home-grown innovation occurs that local businesses and their governments wish to protect, the need for legal principles to protect proprietary information rises. However, due to a number of factors that have gone largely unexplored, not all countries value trade secret protection to the same degree or at the same time. This is partly due to the fact that it was not until fairly recently in the development of trade secret doctrine that trade secrets could be treated as a form of property, let alone a form of intellectual property. Additionally, as the law governing the protection of proprietary information develops in a given country, the legal theories and processes that are used to protect such information vary.

1.47 The varied development and details of international law with respect to trade secrets is not unlike the history of trade secret law in the United States, which provides an example of legal norm-making and how the process can often take decades to reach fruition.[35] It is generally recognized that the first trade secret case was decided in the United States in 1837,[36] but it was not until 1979 that a proposed uniform law was approved with the goal of harmonizing trade secret law throughout the United States.[37] Even after the adoption of the UTSA in 1979, it was not until 1988 that the majority of US states enacted the UTSA.

1.48 Much like the state of international trade secret protection today, for over 150 years between 1837 and 1988, the law governing trade secrets in the United States was primarily based upon a number of different theories (including tort, contract, property, unfair competition and equitable theories) and application of trade secret doctrine, such as it was, was marked by inconsistency and unpredictability. This confusing and unpredictable state of affairs was the principal

34 Catherine Fisk, *Working Knowledge: Employee Innovation and the Rise of Corporate Intellectual Property, 1800–1930* (2009).

35 Sandeen, n. 6 above.

36 See *Vickery* v. *Welch*, 36 Mass. 523 (1837).

37 Uniform Trade Secrets Act (1985).

impetus behind the efforts of the American Bar Association and its members to draft a uniform law to govern trade secrets.

1.49 Current efforts to expand and harmonize trade secret protection on an international scale can be seen as a repeat of the process that the United States followed, but on a much larger scale. The first step in that process was accomplished in 1994 when WTO member countries officially agreed to provide a minimal degree of protection for undisclosed information (aka trade secrets) as set forth in Article 39 of the TRIPS Agreement. The next step is to have the countries of the world adopt a more detailed and harmonized understanding of the scope and limits of trade secret protection, including increased enforcement efforts.

1.50 Historically, when harmonization of IPRs has been deemed necessary, the international community has developed multilateral agreements that, over time, have become more specific and detailed. This can be seen in the various amendments to the Paris Convention and the Berne Convention and, more recently, in the detailed provisions of the TRIPS Agreement with respect to patent law, copyright law and trademark law.[38] Thus, while the TRIPS Agreement still allows WTO member countries numerous 'flexibilities' concerning the details of their intellectual property laws,[39] more standards are specified in TRIPS than are contained in earlier multilateral agreements.

1.51 Since the TRIPS Agreement was adopted more than 20 years ago, there has been little effort to amend it except with respect to the issue of access to pharmaceuticals as reflected in the Doha Agreement. Instead, where weaknesses have been perceived in the protection for IPRs, both the United States and EU (as well as their allies) have pursued what is referred to by some as a 'TRIPS-plus' strategy designed to ratchet-up the protection for IPRs through a series of bilateral or regional trade agreements or through organizations outside of the WTO. In this way, international norm-making is achieved over time in a piecemeal fashion between a small number of countries rather than as a product of collective decision-making and consensus by a large number of countries.

1.52 Efforts to require more details and enforcement with respect to trade secret rights are following the piecemeal method of international norm-making, at least for now. Rather, than negotiating an amendment to the TRIPS Agreement or a new multilateral agreement regarding trade secrets, greater trade

38 See e.g., Paris Convention, Art. 6*bis*; Berne Convention, Art. 2*bis*; TRIPS Agreement, Part II: Standards Concerning the Availability, Scope and Use of Intellectual Property Rights.

39 See Sandeen, n 2 above.

secret harmonization is being pursued through a series of initiatives, including the proposed EU Trade Secret Directive, the proposed Trans-Atlantic Trade and Investment Partnership[40] and the proposed Trans-Pacific Partnership Agreement.[41]

1.53 It is an interesting time to practise in the area of trade secret law and this book aims to help make the efforts of attorneys and their clients to identify, protect and enforce trade secret rights throughout the world more efficient and successful.

40 European Commission, Transatlantic Trade and Investment Partnership, available at http://ec.europa.eu/trade/policy/in-focus/ttip/.

41 See Trans-Pacific Partnership Agreement, n. 31 above.

2

ARTICLE 39 OF THE TRIPS AGREEMENT

I. SIGNIFICANCE OF THE WTO AGREEMENT

2.01 As noted in Chapter 1, the first effort to harmonize international trade secret principles occurred as part of the negotiations that led to the creation of the World Trade Organization (WTO) when the Agreement on Trade-Related Aspects of Intellectual Property ('TRIPS Agreement')[1] was included as an annex (or appendix) to the broader WTO Agreement.[2]

2.02 For those unfamiliar with the history and purpose of the TRIPS Agreement, it is important to first understand the significance of its inclusion as an annex to the agreement that created the WTO. As has been noted repeatedly elsewhere, one of the most important features (if not the most important feature) of the WTO Agreement is that it includes enforcement provisions that allow WTO member countries to bring actions against other countries that they contend are not in compliance with the terms of the WTO Agreement. This is done pursuant to a prescribed dispute settlement process that has several stages and can result in an enforceable finding of non-compliance.[3]

2.03 Any WTO member country that does not comply with the provisions of Article 39 of the TRIPS Agreement may be subjected to the WTO Agreement's dispute settlement process and, ultimately, may be required to correct its laws. Unfortunately for companies and their attorneys who wish to do business in a country with trade secret laws that are perceived to be weak or non-existent,

1 Agreement on Trade-Related Aspects of Intellectual Property Rights, Annex 1C, Legal Instruments, Results of the Uruguay Round, vol. 31, 33 ILM 81 (1994).

2 Marrakesh Agreement Establishing the World Trade Organization, 15 April 1994.

3 *Ibid*., Dispute Settlement Understanding, Annex 2.

this process is of little solace, but at least it ensures that some trade secrecy related legal principles are likely to exist in each WTO member country.

A. General provisions of the TRIPS Agreement

2.04 Apart from using the WTO dispute settlement process to resolve disputes between countries, there are several general provisions of the TRIPS Agreement that are crucial for an understanding of the proper scope and application of Article 39, the provision governing 'undisclosed information'. First, is the principle of national treatment that is expressed in Article 3 of the TRIPS Agreement. Pursuant to this principle, although the TRIPS Agreement does not require perfect harmonization of the laws of WTO member countries, (with few exceptions) it requires all WTO member countries to accord the nationals of other WTO countries treatment 'no less favourable than it accords to its own nationals with regard to the protection of intellectual property'. Thus, as applied to trade secret laws, WTO member countries cannot have one set of trade secret laws to protect domestic companies and another set of trade secret laws to protect foreign companies.

2.05 The second general provision of the TRIPS Agreement that may affect the scope of trade secret laws in force in WTO member countries is the 'most favoured nation' provision of Article 4. It provides that: 'any advantage, favour, privilege or immunity granted by a Member to the nationals of any other country shall be accorded immediately and unconditionally to the nationals of all other Members'. In other words, WTO member countries are (with some exceptions) precluded from treating one trading partner better than another. This is significant with respect to bilateral or multilateral Free Trade Agreements (FTAs), discussed below, which are often used to ratchet-up intellectual property protection because, once they are entered into by a country, Article 4 of the TRIPS Agreement requires that the nationals of any WTO member country be provided that same protection.

2.06 Article 8 of the TRIPS Agreement sets forth two express provisions that WTO member countries may use to justify restrictions on the scope and enforcement of trade secret laws. Article 8.1 provides that countries can 'adopt measures necessary to protect public health and nutrition, and to promote the public interest in sectors of vital importance to their socio-economic and technological development'. Article 8.2 allows countries to adopt measures 'to prevent the abuse of intellectual property rights by rights holders or the resort to practices which unreasonably restrain trade or adversely affect the international transfer of technology'. Both of the foregoing provisions come with the important

caveat that such measures must be 'consistent with the provisions of this Agreement'.

B. Enforcement requirements in the TRIPS Agreement

2.07 Part III of the TRIPS Agreement (Articles 41 through 61) is a generally applicable provision that sets forth fairly detailed requirements concerning the enforcement of intellectual property rights (IPRs) (arguably including trade secrets) by WTO member countries. It differs from the aforementioned state-to-state dispute settlement process because it concerns the measures that must be put in place by WTO member countries so that IPR owners can enforce their rights against alleged infringers and misappropriators. The basic requirement is that WTO member countries 'shall ensure that enforcement procedures that are specified in this Part are available under their law so as to permit effective action against any act of infringement of intellectual property rights covered by this Agreement'. It then proceeds to detail general principles of due process, rules of evidence, available remedies and other matters that each WTO member country must implement.

2.08 While Part III of the TRIPS Agreement is subject to interpretation and implementation by each WTO member country and contains a lot of flexibility, it provides attorneys with a useful guide to the types of enforcement procedures that should be available in each WTO member country. As further discussed in Chapter 6 and in Part II, the available enforcement procedures may take the form of civil, administrative or criminal proceedings.

2.09 Article 41 of the TRIPS Agreement sets forth general principles that are required for IPR enforcement. In the order that they are presented, these include:

(a) expeditious remedies to prevent infringement;
(b) remedies which constitute a deterrent to further infringements;
(c) fair and equitable procedures;
(d) decisions on the merits that, preferably, are written and reasoned;
(e) decisions on the merits that are based only on evidence in respect of which parties were offered the opportunity to be heard; and
(f) an opportunity for judicial review of administrative decisions, except for acquittals in criminal cases.

Significantly, Article 41.5 states that there is no requirement for WTO member countries to establish judicial systems that are specifically designed for the

enforcement of IPRs or to dedicate more resources to IPR enforcement than to the enforcement of laws generally.

2.10 Article 42 of the TRIPS Agreement provides more details regarding the fair and equitable procedures that are required, including adequate notice of the claims against a defendant, the right to legal counsel and the requirement of evidence to support claims and defences. It also provides that the applicable procedures 'shall provide a means to identify and protect confidential information unless this would be contrary to existing constitutional requirements'. This last provision is particularly important to trade secret litigants who risk the loss of trade secrecy as a result of enforcement procedures and is a major focus of trade secret harmonization efforts.

2.11 Article 43 of the TRIPS Agreement addresses the issue of evidence in more detail by requiring judicial authorities (under specified conditions) to require an opposing party to produce relevant evidence concerning the claims. Significantly, it does not go so far as to require US-style discovery, but at least there is some requirement of disclosure coupled with possible sanctions to compel compliance with whatever discovery the judicial authorities deem appropriate.

2.12 Articles 44 through 46 of the TRIPS Agreement specify the types of remedies that must be available following a finding of IPR infringement. These include injunctive relief, damages, attorney's fees and the possible destruction of infringing goods. Significantly, however, both Articles 44 (injunctions) and 45 (damages) specify knowledge requirements that may limit the availability of remedies, particularly with respect to third parties who come to possess infringing goods or misappropriate trade secrets.

2.13 Article 47 is an optional provision that allows WTO member countries to 'provide that judicial authorities shall have the authority … to order the infringer to inform the right holder of the identity of third persons' who are involved in infringing activity. Article 48 provides that judicial authorities shall have the authority to order the indemnification of a defendant who is wrongfully enjoined and to award attorney's fees to a prevailing defendant.

2.14 Of particular importance to trade secret claims are the provisions of Article 50 of the TRIPS Agreement. It requires that WTO member countries provide 'prompt and effective provisional measures' to prevent infringement and the right to an injunction to prevent irreparable harm and to allow such injunctive relief to be granted '*inaudita altera parte*' (without the presence of the other party). As is further discussed in Chapter 3, in the case of trade secrets, such an

injunction is often needed to prevent the widespread disclosure of trade secrets and the resulting loss of trade secrecy.

2.15 Articles 51 through 60 of the TRIPS Agreement specify special requirements with respect to border measures but explicitly only relate to the suspected importation of 'counterfeit trademark or pirated copyrighted goods', as defined. Thus, whether the required border protection measures which are adopted in each WTO member country also apply to the importation of goods that were made using misappropriated trade secrets will depend upon whether such measures have been voluntarily extended to include trade secret misappropriation claims. An obligation to provide such border measures with respect to trade secrets may also be found in other multilateral or bilateral trade agreements.

2.16 Article 61 of TRIPS is similarly limited to trademark and copyright infringement claims. It requires WTO members to 'provide for criminal procedures and penalties to apply', but only with respect to 'trademark counterfeiting and copyright piracy on a commercial scale'. Thus, it is optional under the TRIPS Agreement for countries to adopt criminal laws to punish trade secret misappropriation, and no part of the TRIPS Agreement details the required elements of a criminal trade secret violation. The more recent trade agreements proposed between various countries seek to require criminal sanctions with respect to some acts of trade secret misappropriation.[4]

2.17 Although Article 39 is part of the TRIPS Agreement, there is some question (or at least some ambiguity) whether Part III of the TRIPS Agreement applies to Article 39. This is because Part III refers to the 'enforcement of intellectual property rights covered by this agreement' and there is a plausible argument based upon the drafting history of Article 39 that trade secrets are not a form of 'intellectual property' as defined in the TRIPS Agreement. However, while the developing world fought hard not to label trade secrets as a form of IPRs in Article 39, Article 1.2 provides that 'the term "intellectual property" refers to all categories of intellectual property that are the subject of Section 1 through 7 of Part II'. The ambiguity that is created is whether Article 1.2 applies to all matter covered in Sections 1 through 7 or only to matter that is labelled as 'intellectual property' within each of those sections.

4 See e.g., United States Trade Representative *et al.*, Trans-Pacific Partnership Agreement (TTP) (2013), available at www.eff.org/issues/tpp.

II. DRAFTING HISTORY OF ARTICLE 39

2.18 The drafting process that ultimately led to the adoption of the TRIPS Agreement and Article 39 was lengthy and took many twists and turns.[5] The first issue that the relevant negotiating group (NG11) confronted was whether IPRs should be addressed in the WTO Agreement at all.

2.19 Based upon a strategy that had been devised by representatives of IP-dependent industries (including representatives of the entertainment and pharmaceutical industries), the US negotiators were quick to argue that the protection of IPRs was essential for free trade and economic development. Other countries, principally India and Brazil, argued that the TRIPS Agreement should not be used as a means to strengthen IPRs but, instead, should focus on how IPRs affect (and can hamper) free trade. The concern was (and is) that greater protection of IPRs would be used as a back-door means of restricting free trade.

2.20 Consistent with the overall goal of tying the protection of IPRs to trade, early proposals by the United States advocated for international standards to protect all forms of IPRs, including trade secrets. In a submission during the first year of meetings of NG11 in 1987, for instance, the Office of the United States Trade Representative detailed its proposed negotiating objectives with respect to trade secrets as follows:

> Trade secrets should be broadly defined to include undisclosed valuable business, commercial, technical or other proprietary data as well as technical information. Misappropriation, including the unauthorized acquisition, use or disclosure of a trade secret, must be prevented. Trade secrets submitted to governments as a requirement to do business shall not be disclosed except in extreme circumstances involving national emergencies or, in the case of public health and safety, provided that such disclosure does not impair actual or potential markets of the submitter or the value of the submitted trade secrets.

While the foregoing contains a cursory sketch of trade secrecy concepts based upon US law, three particular trade secret issues emerged in the year after the USTR's initial pronouncement.[6] The first involved the definition of misappropriation and the conditions under which it might be presumed. Second, was the

---

5 For a detailed account of this drafting history, see Sharon K. Sandeen, 'The Limits of Trade Secret Law: Article 39 of the TRIPS Agreement and the Uniform Trade Secrets Act on Which It is Based' in Rochelle C. Dreyfuss and Katherine J. Strandburg (eds), *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research* (2011), p. 537. The information that follows in the text provides a summary.

6 Rudolf Krasser, 'The Protection of Trade Secrets in the TRIPS Agreement' in Friedrich-Karl Beier and Gerhard Schricker (eds), *From GATT to TRIPS: The Agreement on Trade-Related Aspects of Intellectual Property Rights* (1996), p. 216.

issue whether liability for trade secret misappropriation should be extended to innocent (i.e., unknowing or non-intentional) possessors of trade secret information (generally referred to as 'third parties' throughout this book). The third issue concerned proposed restrictions on the use of trade secrets submitted to governments. As will be seen, all of these issues ended up being addressed in Article 39, but not much else.

2.21 In June 1988, a document titled *Basic Framework of GATT Provisions on Intellectual Property, Statement of Views of the European, Japanese and United States Business Communities* ('*Basic Framework*') was released as the next step in the NG11 negotiating process.[7] While the *Basic Framework* sets forth eight IPR-related principles, only two relate to trade secrecy. Principle 5 states: 'A person who has acquired proprietary information without the consent of the owner shall be effectively deterred from using or disclosing it further when such acquisition was contrary to honest practices in industrial and commercial matters'. Principle 7 details well-established limits on the scope of trade secret protection, including the observation that it does not extend to publicly available information or to information that can be reverse engineered.

2.22 In October 1988, the US negotiators submitted a more detailed proposal for the protection of trade secrets that addressed six topics: (1) the scope of protection; (2) the term of protection; (3) maintenance of rights; (4) the definition of misappropriation; (5) the rights conferred; and (6) conditions of government use.[8] The US proposal also contained a provision requiring the protection of confidential information during enforcement proceedings. Following this submission, however, the work of NG11 stalled due to continuing disagreements about the proper scope of its work.

2.23 When the negotiations of NG11 finally resumed in mid-1989, a new issue arose with respect to trade secrets; namely, whether trade secrets are actually a type of intellectual property. Significantly with respect to present efforts to expand and harmonize international trade secrecy norms, many developing countries resisted efforts by the United States, the EU and Japan to characterize trade secret rights as IPRs.[9] Part of the concern related to the general complaint that IPRs should not be tied directly to trade policy, but it also reflected a concern about attaching a property label to such rights for fear that claims of

---

7 *Statement of Views of the European, Japanese, and United States Business Communities, Basic Framework of GATT Provisions on Intellectual Property*, MTN.GNG/NG11/W/26 (June 1988).

8 Negotiating Group on Trade-Related Aspects of Intellectual Property Rights, *Including Trade in Counterfeit Groups, Suggestion by the United States for Achieving the Negotiating Objective, Revision*, MTN.GNG/NG11/W/14 Rev. (17 October 1988).

9 Sandeen, n. 5 above.

broad, exclusive rights would follow. India argued that trade secrets are not a form of IPR because it viewed trade secret law as a form of unfair competition law and it was unwilling to apply property principles to trade secret misappropriation claims.[10] Ultimately, 14 countries adopted India's position and expressed their unwillingness to negotiate concerning trade secrets, thereby effectively stifling discussion about the appropriate scope and limits of trade secret law.

2.24 The negotiating impasse concerning the proper grounding of trade secret law continued until the actual process of preparing a draft of the TRIPS Agreement began in March 1990. Initially, proposed drafts of a provision regarding trade secrecy were much more detailed than the current language of Article 39 and the United States continued to insist that trade secrets were a form of intellectual property.

2.25 During this period, other points of disagreement emerged as indicated by the bracketed portions of critical drafts. The first concerned the definition of a trade secret; namely, whether trade secret protection should extend to secrets with only potential commercial value (e.g., those secrets that are not yet used or licensed commercially) and whether the protected information should be denominated 'trade secrets' as proposed by the United States, 'proprietary information' as proposed by Switzerland, or 'undisclosed information' as suggested by the EU. Second, issues arose concerning the meaning of misappropriation and the illustrative list of acts 'contrary to honest commercial practices' that was introduced as a footnote in a draft proposed by the United States. Third, questions arose concerning the proper wording and mechanisms for holding third parties liable for trade secret misappropriation. Lastly, there were discussions concerning the 'readily ascertainable' language proposed by the United States and the 'easily accessible' language proposed by the EU.

2.26 Following the breakdown of Uruguay Round negotiations due to disputes over the agricultural provisions of the broader WTO Agreement, the TRIPS negotiations continued in a modified format throughout most of 1991. Ultimately, to move matters toward a final agreement, a stripped-down version of a draft agreement was prepared and presented to countries. As reflected in this final draft, often referred to as the 'Dunkel Draft', the provisions governing trade secrets were reduced to the three sections that are set forth in current Article 39 of the TRIPS Agreement.

10 Communication from India, MTN.GNG/NG11/W/37. para. 46.

2.27 Significantly, the United States did not get everything it had proposed during the TRIPS negotiations. In a crucial compromise, Article 39.1 explicitly states that the protection of 'undisclosed information' arises under pre-existing principles of unfair competition and does not label such information as a form of IPR. The US negotiators also did not succeed in including provisions in Article 39 that would have required countries to institute measures to protect trade secrets during enforcement proceedings, although as noted earlier they are arguably included in the last sentence of Article 42.

III. REQUIREMENTS OF ARTICLE 39

2.28 Article 39 requires all WTO member countries to have laws in place that enable the effective protection of undisclosed information. Specifically, Article 39.1 requires all WTO member countries, 'in the course of ensuring effective protection against unfair competition as provided in Article 10*bis* of the Paris Convention' to provide natural and legal persons 'the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices'.

2.29 Compared to other provisions of the TRIPS Agreement with respect to patents, copyrights and trademarks, Article 39 is sparse on details. In particular, it does not specify the methods by which countries must provide such protection or such common details of civil and criminal actions as the essential elements of a claim or crime and available defences. Although (as detailed above) other provisions of the TRIPS Agreement require civil remedies, those provisions only apply if Part III of the TRIPS Agreement ('Enforcement of Intellectual Property Rights') is interpreted to apply to Article 39 and, in any event, the border measures and criminal provisions of Part III only apply to trademark counterfeiting and copyright piracy.

2.30 In contrast to the multiple provisions of the Uniform Trade Secrets Act (UTSA) (discussed in Chapter 3) and the proposed EU Trade Secret Directive (set out in Appendix 1), Article 39 of the TRIPS Agreement only contains one detailed provision regarding trade secret law and one that relates to data exclusivity. Article 39.2 identifies the wrongful acquisition, disclosure and use of undisclosed information as conduct contrary to honest business practices. It also defines the three requirements for information to be classified as 'undisclosed information' (or trade secrets).

2.31 In language that is nearly identical to the definition of a trade secret under the UTSA (see Chapter 3), Article 39.2 states that information is protectable if it:

(a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
(b) has commercial value because it is secret; and
(c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

Nowhere in Article 39 is the terminology 'generally known', 'readily accessible', 'commercial value' and 'reasonable steps' defined, effectively leaving it up to the legislatures and courts of each country to define those terms.

2.32 Unlike the UTSA which includes a detailed, but not exclusive definition of 'misappropriation' and 'improper means', little effort was made in Article 39 to define what is meant by a 'manner contrary to honest commercial practices'. Once again, it is up to the legislatures and courts of each country to identify acts which are deemed dishonest. Footnote 10 to Article 39.2 does, however, identify the following four acts of dishonest behavior: (1) 'breach of contract' (presumably a contract that promises confidentiality); (2) 'breach of confidence' (presumably an obligation not based upon a contract); (3) 'inducement to breach'; and (4) 'the acquisition of undisclosed information by third parties who knew, or who were grossly negligent in failing to know, that such practices were involved in the acquisition' (referring to the previous three wrongful acts). Significantly, unlike the UTSA, footnote 10 does not contain a broader list of criminal and tortious activities that would constitute misappropriation and 'improper means', leaving those activities to be defined according to what each WTO member country believes is a 'manner contrary to honest business practices'.

2.33 The term of art that is used to describe the information that is the subject of Article 39 is 'undisclosed information' rather than 'trade secrets'. This reflects acceptance of the EU's proposed definition. It also reflects the fact that a broader labelling scheme was needed to cover all three provisions of Article 39, with only the first two having to do with trade secrets.[11] In more recent

11 In an interview with former US Trade Negotiator, Michael Kirk, concerning Art. 39, Sharon Sandeen asked him why the data exclusivity provisions of Art. 39.3 were placed in Art. 39 instead of a separate section. He responded: 'Where else would you put it.' The view was that all provisions regarding undisclosed information should be lumped together in one article. Importantly, this does not mean that all undisclosed information that is discussed in Art. 39 constitutes trade secrets. (See Chapter 8.)

international discourse, it appears that the use of the label 'trade secrets' has become more universally accepted, at least among developed countries, as reflected in the language that is used in many of the laws that have been enacted and the proposed EU Trade Secret Directive.

IV. FLEXIBILITIES OF ARTICLE 39

2.34 At first blush, particularly for countries that are disinclined to protect trade secrets or that are inclined to recognize a need to balance trade secret protection with other important social values, Article 39 may seem onerous. In reality, it provides WTO member countries significant leeway in defining the parameters of trade secret law. This is because WTO member countries can take advantage of the lack of specificity and exercise flexibilities in deciding how best to implement the requirements of Article 39. For instance, while WTO member countries cannot change the definition of undisclosed information, they are free to define what is meant by 'generally known', 'readily accessible' and 'reasonable efforts'. As a result, those definitions may cover more rather than less information and thereby restrict the body of information that can qualify for trade secret protection. Similarly, since Article 39 (like the text of the UTSA) does not set forth any defences to trade secret misappropriation, WTO members are free to do so, although it is clear from the drafting history of Article 39 that reverse engineering and independent development are to be deemed proper activities.[12]

2.35 Article 1.1 of the TRIPS Agreement provides, in pertinent part: 'Members shall be free to determine the appropriate method of implementing the provisions of this Agreement within their own legal system and practice'. Since implementation of Article 39.1 requires WTO member countries to prevent acts 'contrary to honest commercial practices', the implementation of Article 39 also depends upon applicable commercial, cultural and social norms, some of which may be different from those of the United States and EU countries. In other words, what one country might define as dishonest commercial practices may be acceptable behaviour in another country. Thus, until the various WTO countries adopt more specific standards with respect to the protection of trade secrets, companies that wish to engage in trade with other countries while still protecting their trade secrets are well advised to consider the commercial, cultural and social norms of those other countries.

12 Sandeen, n. 5 above.

2.36 In addition to differences in what may be considered dishonest commercial practices, the various WTO member countries (like the various states of the United States) are likely to have different views on countervailing issues (such as antitrust/competition issues, employee mobility concerns and the importance of knowledge diffusion) that may affect the scope of trade secret protection and enforcement. The TRIPS Agreement explicitly recognizes the importance of these countervailing considerations in several provisions. First, Article 7 states that:

> the protection of IPR should contribute to the promotion of technological innovation and the transfer and dissemination of technology, to the mutual advantage of producers and users of technological knowledge and in a manner conducive to social and economic welfare, and a balance of rights and obligations.

Article 8 allows WTO member countries to 'adopt measures necessary to promote the public interest' and 'to prevent the abuse of intellectual property rights by rights holders or the resort to practices which unreasonably restrain trade or adversely affect the international transfer of technology'. Article 73 allows for exceptions with respect to 'essential security concerns' that may be used to limit rights in certain trade secrets, for instance related to fissionable material and the implements of war.

V. METHODS OF COMPLIANCE WITH ARTICLE 39

2.37 As reflected in various sources, including the notifications submitted to the WTO, reports of the Office of the US Trade Representative and the European Commission Study on the *circa* 2012 trade secret laws of various EU countries, the methods that WTO countries use to comply with Article 39 of the TRIPS Agreement can vary widely.[13] Some countries, particularly those that follow the civil law tradition, have adopted specific statutes for the protection of trade secrets. Other civil law countries rely on existing statutes governing unfair competition as the basis for their compliance with Article 39. In common law countries (most notably India), general principles of unfair competition and duties of confidence as developed through the courts are cited as evidence of compliance with Article 39. Other countries rely upon principles of contract law and may require the existence of a contract as the basis for a successful trade secret claim.

13 European Commission, *Study on Trade Secrets and Confidential Business Information in the Internal Market* (2013), pp. 117–48, available at http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_final-study_en.pdf (providing a survey of the EU business enterprise sector).

2.38 Another way to frame the foregoing observation is to say that the state of trade secret protection worldwide is much like the state of trade secret protection in the United States before the widespread adoption of the Uniform Trade Secrets Act in the late 1980s. A variety of theories and processes exist in WTO member countries that may allow for the protection of trade secrets, but whether they result in the timely and effective protection of trade secrets is another question.

2.39 Confronted with the foregoing uncertainty, attorneys are trained to research the applicable law so that they can properly advise their clients about the risks and benefits of a particular business enterprise. However, for a variety of reasons, the laws and court decisions of other countries are not always written down, may not be reported in accessible court decisions and may be spread throughout disparate parts of the written code. This can make it difficult for foreign companies and their attorneys to ascertain details about the applicable law. Article 39 of the TRIPS Agreement at least provides some guideposts.

2.40 As we discuss the trade secret laws of various countries in Chapters 9 and 10, we include relevant information on their adoption and compliance status with TRIPS. We do the same when addressing the UTSA in the United States in Chapter 3 and the proposed EU Trade Secret Directive set out in Appendix 1.

3

US TRADE SECRET LAW AND THE UNIFORM TRADE SECRETS ACT

I. INTRODUCTION: THE UNIFORM LAW-MAKING PROCESS IN THE UNITED STATES

3.01 One of the challenges to understanding trade secret law in the United States relates to the fact that US trade secret law is primarily based upon the laws of each of the 50 states. Because the US government is organized as a federal system with most legislative power (at least in theory) residing in the states, the US Congress has limited powers to adopt laws to regulate activities in individual states. The principal exceptions include the powers granted to the US Congress under the Commerce Clause of the US Constitution 'to regulate commerce among foreign nations, and among the several states, and with Indian tribes'[1] and the provision of the US Constitution that grants Congress

1 US Constitution, art. I, s. 8, cl. 3.

the exclusive power to adopt patent and copyright laws.[2] To date, however, the US Congress has not exercised its Commerce Clause powers to adopt a federal civil trade secret law, relying instead on a combination of well-established state laws and some overarching federal policies.[3]

3.02 Among the 50 states, the harmonization of state laws is achieved through three basic processes: (1) the common law development of the law whereby judges adopt the views of judges from other states and thereby create a 'majority view' on a given point of law; (2) statutory enactments whereby legislators of one state adopt statutes already enacted in other states; and (3) the uniform law-making process whereby an entity drafts and proposes uniform laws for adoption by all 50 states.

3.03 Historically, the common law development of US law (or at least the better reasoned view of the common law) has been detailed in the Restatement series published by the American Law Institute, in reported case decisions and in a variety of treatises. This includes the trade secret provisions of the *Restatement (First) of Torts* that were published in 1939 and the expansion of and updates to those provisions that were published in the *Restatement (Third) of Unfair Competition* in 1995.

3.04 The Uniform Trade Secret Act (UTSA), which is now the predominant trade secret law in the United States, is an example of the third type of harmonized law noted above. It was drafted by the National Conference of Commissioners of Uniform State Laws (NCCUSL, but now known as the Uniform Law Commission) over a period of over 12 years beginning in the late 1960s and ending in 1979.[4] Since then, NCCUSL has successfully advocated for the adoption of the UTSA by 47 of the 50 states. The UTSA is also the governing law in the District of Columbia, the US Virgin Islands and Puerto Rico.

3.05 In the states that have yet to adopt the UTSA (as of early 2015: New York, North Carolina and Massachusetts), significant harmonization of trade secret principles has been achieved through the other two processes noted above.

---

2 U.S. Constitution, art. I, s. 8, cl. 8.

3 Proposals to enact a federal civil cause of action for trade secret misappropriation have been frequently introduced in the US Congress in recent years and, thus, sole reliance on state law may change in the future. Typically, however, these proposals do not pre-empt state trade secret law and are modelled after the Uniform Trade Secrets Act (UTSA).

4 For a detailed history of the UTSA, see Sharon K. Sandeen, 'The Evolution of Trade Secret Law and Why Courts Commit Error When They Do Not Follow the Uniform Trade Secrets Act' (2010) 33 *Hamline L. Rev.* 493, reproduced in Sharon K. Sandeen and Elizabeth A. Rowe (eds), *Trade Secrets and Undisclosed Information* (2014). For a more detailed examination of US trade secret law, see Sharon K. Sandeen and Elizabeth A. Rowe, *Trade Secret Law in a Nutshell* (2013).

North Carolina adopted a statute which, while not identical to the UTSA, is substantially similar. Both New York and Massachusetts have yet to formally adopt the UTSA, but the common law development of the law in those states is largely in line with the provisions of the UTSA, particularly to the extent that the *Restatement (Third) of Unfair Competition* is relied upon for an understanding of applicable law.

3.06 Of course, in all states (and all countries), absolute harmonization cannot be assumed as minor differences in the wording and application of various legal principles may exist. For instance, with respect to the UTSA, some states adopted the original 1979 version of the UTSA, while others have adopted the amended 1985 version of the UTSA. In addition, ancillary doctrines of law are often applied in trade secret cases, such as the laws governing restraints on trade and the employment relationship, as discussed in Chapters 4 and 5.

3.07 As with the individual trade secret laws of each country (see Chapters 9 and 10), the individual laws and case decisions of the various US states must be consulted to determine the true scope and limits of trade secret law as applied in each state. However, both the details of the UTSA and the issues that it raises provide a good foundation for understanding US trade secret law, as well as the laws of other countries that use it as a model for their laws.

II. TRADE SECRET SUBJECT MATTER

3.08 Under the UTSA, the theoretical scope of trade secret protection is very broad because it can apply to 'any information' that meets the three requirements for trade secrecy, discussed below. This can include technical information that could be the subject of a patent application or non-technical business information, such as a customer list or business plans. The illustrative types of potential trade secret information listed in the UTSA include a 'formula, pattern, compilation, program, device, method, technique or process', but this list is not meant to be exclusive.

3.09 Before the adoption of the UTSA, the common law of the United States as expressed in the *Restatement (First) of Torts* (and applicable in most states until the adoption of the UTSA in a given state) required that for information to be protected as a trade secret it must be used in one's business.[5] This prevented valuable information that was not yet in commercial use and so-called 'negative information' from being protected as a trade secret. The definition of a trade

5 *Restatement (First) of Torts* (1939), s. 757.

secret under the UTSA eliminates these limitations while still requiring the information to be of commercial value. As a consequence, both negative information and information with only a potential independent economic value can be protected under the UTSA.

3.10 Although the drafters of the UTSA debated whether trade secret information should exist in a tangible form before it could be protected as a trade secret, there is no tangibility requirement under the UTSA. This means that trade secrets may only exist in someone's mind. As a practical matter, however, it is difficult to prove that information has been wrongly acquired if it has never been fixed in a tangible form or otherwise shared. Additionally, as is discussed in Chapter 5, ownership issues can arise with respect to any information that is developed by and held in the minds of employees.

III. REQUIREMENTS FOR TRADE SECRET PROTECTION

3.11 As currently drafted, the UTSA contains 12 sections but the most important section is section 1 which defines a 'trade secret' and 'misappropriation', among other things. In contrast to the flexible and amorphous common law definition of a trade secret that was developed at common law and that is described in the commentary to section 757 of *Restatement (First) of Torts*, section 1(4) of the UTSA provides:

> 'Trade secret' means information, including a formula, pattern, compilation, program, device, method, technique, or process that:
>
> (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and
> (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

From the foregoing, it is generally recognized that there are three requirements for trade secrecy under the UTSA. First and foremost, the information must be secret in the sense that it is not generally known or readily ascertainable. Second, the information must have independent economic value (sometimes referred to as 'commercial' value) that is derived, not from the inherent value of the information, but from the fact that the information is secret. Lastly, the information must be subject to reasonable efforts to maintain its secrecy.

3.12 The foregoing definition is nearly word for word identical to the definition of a trade secret that is set forth in Article 39.2 of the TRIPS Agreement, making it

clear that the UTSA was the source for that definition. The principal exceptions are that Article 39.2 uses the terms 'readily accessible' instead of 'readily ascertainable', 'commercial value' instead of 'economic value' and 'reasonable steps' instead of 'reasonable efforts'. Additionally, Article 39.2 contains some language that, while consistent with US trade secret law, is not contained in section 1 of the UTSA. Specifically, Article 39.2(a) (in defining secrecy) includes the language 'in the sense that it is not, as a body or in the precise configuration and assembly of its components … ', presumably to recognize the combination trade secret theory of US law (discussed below). Also, the definition of reasonable steps in Article 39.2(c) contains the language 'by the person lawfully in control of the information'.

3.13 From the foregoing, it can be seen that trade secret law does not protect all information or even all 'business and proprietary information'. While the theoretical definition of a trade secret is broad and can cover a wide variety of information in a number of forms, to be a protectable trade secret the information that a business thinks is important proprietary information must meet the precise requirements of the UTSA. Information that does not meet the definition of a trade secret may be kept confidential by its owner, but if such information leaks out or is wrongfully acquired by another, there is no actionable trade secret claim.

A. Secrecy

3.14 As numerous US cases have recognized, secrecy is the *sine qua non* of trade secret protection. Without it there are no trade secrets, regardless of the amount of time, money and effort that a business spent to develop and protect its information. In the United States, whether information is generally known or readily ascertainable (and, therefore, not secret) is a question of fact that, as a practical matter, can only be determined during trade secret litigation.

3.15 Unlike patent rights, there is no need for trade secret rights to be 'granted' by an authority of the government and trade secrets cannot be 'registered' like copyrights and trademarks. Information either meets the requirements for protection or it does not, but the status of such information will generally not be tested until a defendant in a trade secret misappropriation claim makes the secrecy of the information an issue. Thus, it is possible for businesses that are unaware of the state of knowledge in a particular field to assert the existence of trade secrets when, in fact, the information is generally known or readily ascertainable.

3.16 Generally, the process that should be followed to prove that a particular body of information is secret (not generally known or readily ascertainable) is similar to a prior art search that is used to determine the novelty and non-obviousness (inventive step) of patentable inventions. Publicly available information is searched to determine both the state of knowledge among the general public and in the particular field. The problem is that, unlike with patented inventions, trade secrets are not necessarily clearly identified by their owners, particularly in a written form or early in the litigation process. Thus, as a practical matter, it is often difficult to determine which prior art is relevant. Also, unlike patent law which looks at prior art as of the time that a patent application is filed, the relevant prior art in trade secret cases extends from the alleged development of the trade secret to the present because trade secrets can cease to exist at any time.

3.17 Assuming that the alleged trade secrets are identified with sufficient specificity and a body of relevant prior art is identified, trade secrecy does not exist for information that is already publicly known at the time of its development by the trade secret owner or that becomes publicly known thereafter. As explained in the commentary to the UTSA, information is generally known if it is both known to the general public and known within a particular industry.[6] The key is whether the principal persons or companies that could obtain economic benefit from the information are already aware of it. For instance, even if a method of drilling for oil is not generally known by members of the public, it cannot be a trade secret if it is generally known among oil drilling companies.

3.18 The readily ascertainable language of the UTSA relates to the difference between what is currently 'known' by the general public or within an industry and what is 'knowable'. Even if information is not presently known, it cannot be protected as a trade secret if it is knowable without too much time or effort. What amount of time and effort is needed to distinguish between protectable trade secrets and unprotectable business information is generally a matter of argument between litigants and often establishes the dividing line between information that is readily ascertainable (and therefore not a trade secret) and information that was reverse engineered (and therefore not misappropriated). In either case, the plaintiff would not have a viable trade secret claim, but in the first instance it may be easier for a defendant to prevail on a motion for summary judgment.

3.19 The commentary to the UTSA provides that '[i]nformation is readily ascertainable if it is available in trade journals, reference books, or published materials',

6 Uniform Trade Secrets Act (1985) (UTSA), s. 1, comment.

but this is not intended as an exclusive list.[7] The information may also be readily ascertainable from goods and services that are placed in the market and from published patents and patent applications. Unlike US patent law (until it was recently amended), there is no provision of the UTSA that distinguishes between published and unpublished knowledge or that limits generally known or readily ascertainable information to information that is located in the United States. However, as a practical matter it may be difficult and costly to identify generally known and readily ascertainable knowledge that is located outside of the United States.

3.20 In the same way that information that exists only in someone's head can be a trade secret under US law, trade secrecy destroying prior art can exist in someone's head or in business practices without ever having been put in tangible form. The challenge in such cases is to find witnesses who can credibly testify to the state of public knowledge of the information. In this regard, it is possible under US law for more than one individual or company to hold the same information as a trade secret so long as it has not reached a point where the information is considered generally known or readily ascertainable.

3.21 An unwritten (at least in the text of the UTSA) and often overlooked restriction on the scope of trade secret protection in the United States concerns what is referred to as 'general skill and knowledge'. Consistent with the laudable goals of knowledge diffusion, education and personal growth, it is generally recognized in the United States that trade secret protection is not available for information that is within the general skill and knowledge of a person who works in a particular field of endeavour, even if such information is not generally known or readily ascertainable.[8] This includes the general skill and knowledge that employees gain while employed with a specific employer even if the nature of the employment is highly technical.

3.22 For example, a new computer programmer who starts her career at Microsoft should not be prevented from using the general skill and knowledge she gained about computer programming in her subsequent employment at Apple. Similarly, a young machinist who is taught and mentored by a more senior worker is allowed to keep and use the wisdom and insights gained thereby. Where the line is drawn between general skill and knowledge and protectable trade secret information is a matter for debate between litigants, but the issue generally focuses on the special qualities and 'uniqueness' of the alleged trade secret information.

---

7 *Ibid.*

8 *See e.g.*, *S.I. Handling Systems, Inc.* v. *Heisley*, 753 F.2d 1244, 1267 (3rd Cir. 1985) (Adams J, concurring).

3.23 Although an alleged trade secret need not meet the strict patent standards of novelty and non-obviousness, some courts expect to see some degree of novelty in the information claimed as a trade secret in order to ensure that trade secret protection is not claimed for information that, based upon public policy, should be free for everyone to use. Conceptually, this type of novelty is part of the generally known and readily ascertainable requirements for trade secrecy and operates to prevent trivial, obvious and low value information from being protected as a trade secret. Often, the inability of an information owner to clearly identify what it considers to be 'special' knowledge, as opposed to general knowledge, is fatal to a claim of trade secrecy.

3.24 As indicated in the UTSA's definition of a trade secret,[9] it is theoretically possible for a person or company to claim trade secret protection in a 'compilation'. However, if the compilation is of a set of known elements, to be protectable as a trade secret something new or unique must be added to or result from the act of compilation. Otherwise the so-called 'combination theory' of trade secrecy would undermine the limits on trade secret protection that are described herein.[10] In particular, the combination theory should not be used to convert information that is generally known or readily ascertainable into protectable trade secrets because it is the strong policy of the United States, as expressed in a number of US Supreme Court cases, that such information is free for anyone to use.[11]

3.25 To successfully claim trade secret protection for a unique combination of known or knowable elements, the information owner should first articulate what is new and different about the combined information and then prove that the combination (as a combination) has independent economic value derived from its secrecy and is the subject of reasonable efforts to maintain its secrecy. For instance, if the combination is a recipe for making cookies, the new and different feature may be the type of eggs or flour that are used, a special 'secret' ingredient, the specific quantity of each ingredient or a combination of all three that results in a unique, unknown and not readily ascertainable recipe.

3.26 The fact that information may be combined in a special or unique way so as to create trade secret information does not mean that all of the combined information is magically transformed into a trade secret. Conceptually (and

---

9 UTSA, s. 1(4).

10 See Tait Graves and Alexander Macgillivray, 'Combination Trade Secrets and the Logic of Intellectual Property' (2004) 20 *Santa Clara Computer and High Tech. LJ* 261.

11 See e.g., *Bonito Boats, Inc.* v. *Thunder Craft Boats, Inc.*, 489 US 141, 162 (1989). The court noted that 'we have consistently reiterated … that ideas, once placed before the public without the protection of a valid patent are subject to appropriation without significant restraint'. *Ibid.* 156.

consistent with similar principles of US patent and copyright law), only the added matter can be protected as a trade secret. For instance, with respect to the above described unique or special recipe, it would be the types of egg and flour, the secret ingredient, and the quantity of each ingredient when combined together that would possibly be protected and not the otherwise known or knowable common ingredients for making cookies.

3.27 Consistent with the foregoing principles, it is clear under US law that trade secrets cannot be created by contract and that contracts cannot be used to restrict the acquisition, disclosure and use of publicly available (known or knowable) information. Rather, for information to be protected as a trade secret, it must have an independent legal existence that meets all of the requirements for protection. Contracts, however, may (and should) be used to establish duties of confidence, but if the underlying information does not meet the definition of a trade secret, there can be no successful trade secret misappropriation claim, but rather a claim relating to the breach of contract.

B. Independent economic value

3.28 The economic value requirement of the UTSA is an under-explored, ill-defined and misunderstood requirement.[12] Those who assert the existence of trade secrets commonly argue that any information that is of value to them or for which they expended time, trouble and money to develop has the requisite 'independent economic value'. However, proving independent economic value it not always that easy because the language of the UTSA seems to require more.

3.29 The language of section 1(4) of the UTSA suggests two aspects of the independent economic value requirement that are often overlooked. First, the information has to 'derive independent economic value because of its secrecy'. In other words, the competitive advantage that the information holder enjoys must be because the information is secret and not because of the inherent value of the information. This concept is included in Article 39.2 of the TRIPS Agreement which requires the putative trade secrets to have commercial value because they are secret.

3.30 Related to the foregoing is the second aspect of the UTSA's definition of independent economic value that arguably limits its scope; namely, the information must be of value 'to others'. Thus, independent economic value should

12 See Eric E. Johnson, 'Trade Secret Subject Matter' (2010) 33 *Hamline L Rev*. 545, reproduced in Sharon K. Sandeen and Elizabeth A. Rowe (eds), *Trade Secrets and Undisclosed Information* (2014).

not exist with respect to information that is unique to the information owner's operations and cannot be used by others because it would not be 'of value to others'. This might include, for instance, information about a company's illegal or tortious activity.

3.31 Although the UTSA uses the term 'economic value' rather than the more common term, 'commercial value', the drafting history of the UTSA suggests that the terms were intended to be synonymous. In some circumstances, however, 'economic value' may be viewed as a broader term which does not require a connection to a commercial or for profit enterprise. This highlights a potential difference between the law of the United States and the laws of other countries; other countries may not extend trade secret protection to non-profit or non-commercial enterprises, particularly since Article 39 of the TRIPS Agreement uses the term 'commercial value'.

C. Reasonable efforts to maintain secrecy

3.32 Due in part to the practical reality that a putative trade secret owner is unlikely to conduct a prior art search for its own alleged trade secrets (discussed above), the reasonable efforts requirement of the UTSA's definition of a trade secret tends to be the focus of many trade secret cases and is the most important requirement in cases where there is no evidence that the subject information is generally known or readily ascertainable.[13] The majority view is that an information owner must take some affirmative steps to protect the putative trade secrets from disclosure, but the number and nature of steps that are 'reasonable' are issues for debate among litigants.

3.33 Because trade secret litigation can be costly and trade secret misappropriation can result in the loss of trade secrecy, the prudent trade secret owner will engage in efforts that are designed to prevent the misappropriation of trade secrets in the first instance. It is only if those efforts are insufficient to secure the actual secrecy of information that the issue of reasonable efforts arises. Unfortunately, because what constitutes 'reasonable efforts' depends upon the circumstances of each case, it can be difficult for a business to predict in advance if they did enough.

3.34 Courts in the United States look at a number of factors to determine the reasonableness of secrecy efforts, including the nature of the trade secrets, the

13 See generally, Robert G. Bone, 'Trade Secrecy, Innovation and the Requirement of Reasonable Secrecy Precautions', in Rochelle C. Dreyfuss and Katherine J. Strandburg (eds), *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research* (2011), p. 537.

location and manner of their storage, the risks of misappropriation and the availability and costs of protection measures. It is clear under US law that extraordinary measures are not needed to meet the reasonable efforts requirement,[14] but at a minimum such efforts should include the identification of the putative trade secret information and some effort to limit access to that information. What, if anything, is required between these two extremes will be decided by the trier of fact and is often influenced by the egregiousness of the alleged misappropriator's behaviour.

3.35 Typical secrecy efforts include: keeping the subject information under lock and key or in encrypted and password protected electronic files; limiting the disclosure and use of the information both internally within the company and externally with business associates; educating employees about the existence and proper handling of the information; limiting access to company facilities; and obtaining express written confidentiality agreements.

3.36 When trade secrets are going to be shared with another, including employees and business associates, special attention must be paid to how the information is handled. The general rule under US law (labelled the third party doctrine of trade secret law) is that the trade secret status of information is lost if the individual or company that is given access to trade secrets is not first placed under an express or implied duty of confidentiality to maintain the secrecy of identified information.[15] One of the purposes of this requirement is to put others on notice of the existence of trade secrets as a prelude to establishing a duty of confidentiality.

3.37 Although theories exist under US law to establish an implied duty of confidentiality in some circumstances, discussed below, the best practice is to obtain a written confidentiality agreement from all companies and individuals who will be given access to trade secrets. The scope, nature and enforceability of these agreements are explained in greater detail in Chapters 4 and 5.

IV. DEFINITION OF MISAPPROPRIATION

3.38 In order to state a claim for trade secret misappropriation in the United States, the plaintiff must plead and prove (1) ownership of (2) one or more trade

14 *E.I. DuPont deNemours & Co.* v. *Christopher*, 431 F.2d 1012 (5th Cir. 1970).

15 See Sharon K. Sandeen, 'Lost in the Cloud: Information Flows and the Implications of Cloud Computing for Trade Secret Protection' (2014) 19 *Va. JL and Tech.* 1.

secrets, (3) some act(s) of misappropriation by the defendant and (4) entitlement to a remedy due to some actual or threatened harm. At common law in the United States (and in the United Kingdom), the definition of misappropriation focused on the alleged wrongful use or disclosure of trade secrets. The UTSA definition of misappropriation explicitly adds the wrongful acquisition of trade secrets to the list of possible wrongdoing.[16] The UTSA also modified common law by more clearly defining situations where an 'innocent' or 'accidental' acquirer of trade secrets (a third party) can be held liable for trade secret misappropriation.

A. Types of wrongdoing

3.39 The definition of misappropriation that is contained in section 1(2) of the UTSA is long and convoluted, partly because the definition is designed to deal both with the case of a direct misappropriator and situations where a third party comes to possess trade secrets that were initially misappropriated by another. Broken down into its various parts, there are three acts related to the treatment of the subject trade secrets that may subject an individual or company to liability for trade secret misappropriation, and three methods of wrongdoing.

3.40 Under the UTSA, misappropriation is defined as the wrongful (1) acquisition, (2) disclosure or (3) use of trade secrets. The methods of wrongdoing are acquisition of trade secrets by 'improper means' and disclosure or use in violation of a valid and enforceable duty of confidentiality. Subsection (C) of section 1(2) of the UTSA defines a third method of wrongdoing as the acquisition of a trade secret by accident or mistake, provided that 'before a material change in position' the acquirer knew or had reason to know that knowledge of the trade secret was by accident or mistake.

3.41 Many of the foregoing concepts are suggested in Article 39 of the TRIPS Agreement, but footnote 10 contains a definition of misappropriation that is at once similar and different from the UTSA's definition. First, the word 'misappropriation' is replaced with the broader and more amorphous phrase 'a manner contrary to honest business practices'. Then, similar to the breach of confidentiality prong of the UTSA, it defines such practices to include 'breach of contract, breach of confidence and inducement to breach'. Also, footnote 10, like the definition of misappropriation under the UTSA, explicitly seeks to impose trade secret liability on third parties (individuals and companies that receive trade secrets from a direct misappropriator) if they 'knew, or were grossly

16 UTSA, s. 1(2).

negligent in failing to know' that dishonest commercial practices were used to acquire the trade secrets.

3.42 The extension of potential trade secret liability to third parties is an important aspect of the USTA because it demonstrates one of the values of a civil trade secret claim over a claim for breach of a confidentiality agreement. The contract principle of privity of contract precludes suing a person who is not a party to the contract and, thus, would not allow a breach of contract claim to be brought against a person who acquired trade secrets from a party to the confidentiality agreement. The definition of misappropriation under the UTSA extends to such cases, provided that the third party had the requisite state of mind.

B. Improper means

3.43 The wrongful acquisition prong of the definition of misappropriation focuses on actions that are designed to acquire trade secrets from a trade secret owner without his consent.[17] Theoretically, this could include a number of behaviours, but under the UTSA wrongful acquisition is defined to mean the use of 'improper means' to acquire trade secrets.

3.44 Improper means is defined in section 1(1) of the UTSA to include criminal and tortious behavior as well as breach of a duty of confidentiality. The specific 'improper' means listed in the UTSA are theft, bribery and espionage, and do not include actions that are deemed proper, as discussed below. Unlike the definition of misappropriation under the UTSA, footnote 10 of Article 39 does not include either the term 'improper means' or a definition, leaving such means to be defined (or not) as a practice 'contrary to honest business practices'.

3.45 Pursuant to case law recognized in most US states, the definition of improper means under the UTSA and at common law is not necessarily limited to activities that would constitute a recognized tort or crime, but could include any actions inconsistent with ethical business practices. In this way, US law is similar to Article 39 of the TRIPS Agreement in allowing for all manner of dishonest commercial practices to count as improper means in accordance with applicable commercial, social and cultural norms. For instance, in the oft-cited case of *E.I. DuPont* v. *Christopher*, the court found that it was contrary to honest businesses practices in Texas for the defendants to take aerial photographs of a manufacturing plant under construction, even though there were no laws to prevent such activity.[18] A key factor in the court's reasoning was that it would

17 *Ibid.* s. 1(2)(i).

18 *E.I. DuPont*, 431 F.2d, n. 14 above, at 1015.

have been wasteful and too costly to require DuPont to obscure a plant that was under construction.

3.46 As a counterpoint to the foregoing, it is generally recognized in the United States that efforts by companies to research the activities of their competitors are pro-competitive because such efforts can lead to better products and services and lower prices for consumers. However, determining where and how to draw the line between actionable 'improper means' of acquiring information about a competitor and 'proper' competitive research is critical. Generally, the public availability and ready ascertainability of information is an important factor. Breaking into facilities (including computer systems) that are not otherwise open to the public is likely to constitute a tort or a crime or otherwise be considered 'improper'. For more information on competitive research (or intelligence), see Chapter 4.

C. Breach of a duty of confidentiality

3.47 The second and third types of wrongful acts under the UTSA (wrongful disclosure or use) can arise in two situations.[19] First, as discussed above, it can occur when trade secret information is first acquired improperly and is then disclosed or used by the direct misappropriator or a third party who knew or had reason to know that the information was trade secret information that was acquired by improper means. The second and more typical disclosure or use scenario involves the proper acquisition of trade secrets from the trade secret owner followed by a disclosure or use of the trade secret in violation of an enforceable duty of confidentiality. The second scenario can occur in an employment relationship or in a business-to-business relationship, provided there is an express or implied duty of confidentiality.

3.48 Under US law (and in keeping with the disclosure purpose of trade secret law discussed in Chapter 1), it is generally recognized that trade secret protection is not lost for information that is kept 'relatively secret' pursuant to an obligation of confidentiality. However, such an obligation must typically be established before the disclosure of the trade secrets and both the existence of putative trade secrets and the desire for confidentiality must be appreciated by the recipient of the information.

3.49 The UTSA does not specify how or when duties of confidentiality arise for the purpose of trade secret law. In the United States, whether or not a duty of

19 UTSA, s. 1(2)(ii).

confidentiality exists that can serve as the basis of a trade secret misappropriation claim is largely a function of common law principles, as summarized in the *Restatement (Third) of Unfair Competition*.[20] Duties of confidentiality may also arise in the United States with respect to certain trust or fiduciary relationships or pursuant to a statute. For instance, attorneys and physicians in the United States owe a general duty of confidentiality to their clients and patients.

3.50 Pursuant to general principles of the common law of contracts in the United States, there are three ways that a duty of confidentiality can arise.[21] First, a duty of confidentiality can arise pursuant to an express promise that is either written or oral. Second, a duty of confidentiality may be 'implied in fact' from the circumstances. In essence, it is possible for an agreement of the parties to be found even if it is not clearly expressed. Finally, in the absence of a contractual obligation that is either expressed or implied, a duty of confidentiality may be 'implied at law' based upon the equities of the situation.

3.51 How easy it is for an implied duty of confidentiality to be found for purposes of trade secret law is an issue of debate among litigants. Some cases in the United States have recognized that the mere transfer of confidential information in the context of an arm's length transaction is not sufficient to create an implied duty of confidentiality.[22] But other cases have found an implied duty of confidentiality under similar circumstances. Two issues that are often the focus of such cases are whether the recipient of the information had reason to know of the existence of trade secrets and of the trade secret owner's desire for confidentiality. The sophistication of the trade secret owner and of the recipient of the information also plays a role in the analysis. Generally, the less sophisticated and the lower paid the recipient of information is, the more unlikely it is that an implied duty will be found. On the other hand, where the owner of an idea is the unsophisticated party, an implied duty of confidentiality may arise.

D. Acquisition by accident or mistake

3.52 Until the adoption of the UTSA by most US states, the predominant common law rule was that a person or company who 'innocently acquired' trade secrets could not be liable for trade secret misappropriation. The UTSA altered US law in this respect by specifying that an individual or company can be liable for trade secret misappropriation if at the time they disclose or use the subject information they 'knew or had reason to know' that the information was trade secret

20 *Restatement (Third) of Unfair Competition* (1995), s. 42.

21 See *Reeves* v. *Alyeska Pipeline Services Co.*, 926 P.2d 1130, 1136 (Alaska 1996).

22 See e.g., *Smith* v. *Snap-On Tools Corp.*, 833 F.2d 578 (1987).

information that had been misappropriated by another.[23] With respect to innocent, accidental or mistaken acquisition, the requisite knowledge must attach before 'a material change in position' by the recipient of the information.[24]

E. Required intent

3.53 As the UTSA's definition of misappropriation makes clear (unlike patent, copyright and trademark infringement in the United States which are in the nature of strict liability torts), trade secret misappropriation is in the nature of an intentional tort. The UTSA requires more than mere negligence; it requires that the plaintiff in a trade secret case prove that the defendant knew or had reason to know of the alleged acts of misappropriation and of the existence of a trade secret. This principle is not explicitly incorporated into Article 39 of the TRIPS Agreement, but is suggested by language in footnote 10 which requires a degree of knowledge by third parties who acquire trade secrets from others.

3.54 The intent (or *mens rea*) requirement of US trade secret law raises the question whether there can be secondary (or indirect) liability for trade secret misappropriation under, for instance, a theory of vicarious liability. Arguably, any theory of secondary liability that does not require proof that the defendant had the requisite state of mind is inconsistent with the explicit language of the UTSA which, as discussed below, allows for third party (or secondary) liability in some but not all situations.

F. Third party liability

3.55 One of the concerns that led to the development of trade secret principles in the United States (and that apparently animates international trade secret harmonization efforts) was the difficulty under common law theories of holding individuals and companies that were not directly responsible for the improper acquisition of trade secrets liable for trade secret misappropriation. This was particularly true with respect to the breach of confidentiality theory of liability because it often depends upon the existence of a contract to which the third party is not likely to be a party. Thus, for instance, a confidentiality agreement between a company and an employee would not bind the employee's new employer.

23 UTSA, s. 1(2)(ii)(B).
24 *Ibid.* s. 1(2)(ii)(C).

3.56 The UTSA explicitly solves the problem of how to reach such third parties by defining the wrongful acquisition of trade secrets to include the acquisition of trade secrets under circumstances where the third party knew or had reason to know that the trade secrets were either acquired by improper means or derived from someone who breached a duty of confidentiality.[25] Article 39 of the TRIPS Agreement includes a similar provision but with a heightened knowledge requirement that requires the third party to possess actual knowledge or be grossly negligent in not knowing of the earlier misappropriation.

3.57 Under the UTSA, two key facts must exist to impose liability on third parties. First, the trade secrecy status of the subject information must continue up to the time the information is acquired by the third party. Second, the third party must know or have reason to know that the information is a trade secret that was misappropriated. As noted above, in the event the third party acquired the trade secret information by accident or mistake, it must also be established that the third party did not materially change position in reliance on the belief that the information was innocently acquired.

3.58 Actual evidence of knowledge by the third party is not necessary; circumstantial evidence is sufficient. If the trade secret owner provides notice to the third party in a timely fashion that information in its possession is a trade secret, then third party liability is more likely. In practice, trade secret owners can enhance the possibility of imposing third party liability by placing competitors and other potential defendants on notice of the existence of trade secrets and the potential that such trade secrets were (or are about to be) misappropriated.

3.59 If liability under the third party provisions of the UTSA cannot be proven, then the only recourse against a third party who possesses and threatens to use or disclose trade secrets might be an alternate theory of liability. For instance, a theory of direct liability under tort law may be pursued where the third party engaged in a wrongful act that provides an independent basis for tort liability. A theory of indirect or secondary liability may also be asserted, if applicable. However, unlike patent and copyright law, trade secret law does not have an established doctrinal mechanism for secondary liability, such as contributory infringement.

25 *Ibid.* s. 1(2)(i), (ii)(B).

V. DEFENCES TO TRADE SECRET MISAPPROPRIATION

3.60 The text of the UTSA does not go into much detail about applicable defences to trade secret misappropriation, but both the commentary to the UTSA and applicable case law recognize a number of important defence arguments that serve to limit the effective scope of trade secret protection in the United States. In particular, in addition to attacking plaintiff's *prima facie* case (which as discussed above requires proof of both the existence of a trade secret and an act of misappropriation), the commentary to section 1 of the UTSA establishes that a defendant in a trade secret misappropriation can argue that the acquisition of the alleged trade secrets was by 'proper means'. The types of proper means (which are further discussed below and in Chapter 4), include:

(1) discovery by independent invention;
(2) discovery by reverse engineering;
(3) discovery under a licence from the owner of the trade secret;
(4) observation of the item in public use or on public display;
(5) obtaining the trade secret from public literature.

As further discussed below, other possible defence arguments include assertion of a statute of limitations defence, the preclusion of common law claims pursuant to section 7 of the UTSA, and a defence based upon principles of free speech. Defences based upon the public's interest in the subject information are not unheard of in the United States, but are not well developed.

3.61 Based upon the foregoing list of proper means, as a practical matter, any information that is used internally within a business and not shared widely (including internal manufacturing processes) is easier to protect as a trade secret than other forms of information, unless it is disclosed in a published patent application or an issued patent. This is because it is difficult to properly acquire such information through a search of publicly available information or by way of reverse engineering. As a result, particularly in light of recent changes to US patent law, certain industries are bound to rely more heavily on trade secret protection than patent protection to protect their manufacturing (and other hidden) processes.

3.62 Also, the foregoing list highlights the fact that it is possible for trade secrecy to be lost through no fault of the trade secret owner and at any time during the useful life of the subject information. This could happen, for instance, if a person or company properly acquires the same or similar information through independent development or reverse engineering and subsequently discloses the information to others within the trade or to the general public. Once

information is disclosed in a manner that it becomes generally known or readily ascertainable (regardless of who discloses it), the trade secret status of the information is lost. This is why the trade secrecy status of information is an ongoing issue in trade secret cases and why the length of any issued injunction may be limited.

A. Independent development

3.63 Pursuant to the principle of independent development, it is not only proper for an individual or company to acquire trade secret information through their own research and development efforts, such efforts are encouraged because they are consistent with the incentive rationale of patent and trade secret law. As a consequence, it is possible for more than one individual or company to develop the same or a substantially similar body of information in a phenomenon known as multiple independent (or simultaneous) inventions.

3.64 Under US trade secret law, if the multiple inventors all keep their information secret so that it does not become generally known or readily ascertainable, then the information can be maintained as a trade secret by all, but none of the inventors could successfully sue the others for trade secret misappropriation if the information was developed by each independently. This is because the information was properly acquired by each. At some point, however, enough people will know the information that it will become generally known and, thereby, lose its trade secret status.

3.65 The key to applying the defence of independent development is the degree of independence exercised by the alleged misappropriator. The development of each inventor's body of information cannot be tainted by improperly acquired or used information, which can happen if a former employee of a trade secret owner is involved in the development of the 'new' invention. Thus, to prove independent development, accused misappropriators will often present evidence that their information was developed in a 'clean room' environment where only general skill and knowledge and publicly available information was present and where former employees of the trade secret owner were not allowed to participate.

B. Reverse engineering

3.66 The defence of reverse engineering differs from the defence of independent development because it is dependent upon the alleged misappropriator having access to the trade secret owner's products or services in a manner that allows for a process of study and testing designed to learn the trade secrets. Thus, the

defence typically arises with respect to mass produced products that are widely distributed or services and processes that are visible to the public.

3.67 As noted in the commentary to the UTSA, although reverse engineering is a proper means of acquiring trade secret information, it cannot be tainted with improperly acquired information.[26] Specifically, the commentary states: 'The acquisition of the known product must, of course, also be by fair and honest means, such as purchase of the item in the open market for reverse engineering to be lawful'.

3.68 As further discussed in Chapter 4, one way that trade secret owners attempt to limit the application of the defence of reverse engineering is by including contractual restrictions on reverse engineering in any licences associated with the sale or distribution of mass produced products, for instance, software licences. The inclusion of restrictions on reverse engineering (and sometimes even independent development) in licences raises the question whether the act of reverse engineering is contractually converted into an improper means of acquiring trade secret information or whether such restrictions are void and unenforceable as against public policy. To date, sufficient case law has not developed in the United States to definitively answer this question, although freedom of contracting is generally favoured in the United States.

C. Acquisition from public sources

3.69 As previously noted in the discussion of secrecy, information is not a trade secret in the first instance if it is generally known or readily ascertainable, but even in cases where information is not found to be generally known or readily ascertainable, a defendant in a trade secret misappropriation case can argue that he acquired his knowledge from public sources. In other words, the focus of this argument is not on the nature of the information acquired, but on the manner of its acquisition.

3.70 Logically, the public sources cited by a defendant who claims that he acquired information from public sources would not be readily ascertainable, otherwise there would be no trade secrets. In practice, however, courts are not always careful to determine the trade secret status of information before requiring the defendant to assert a defence. Thus, it is often the case that an argument of acquisition from public sources has to be made by the defendant.

---

26 *Ibid.* s. 1 comment.

3.71 Conceptually, the argument of acquisition from public sources is similar to the argument of reverse engineering in that they are both dependent upon the availability of public (although sometimes obscure) information. The difference between the two focuses on the degree to which the trade secrets are revealed by the public information and whether the information can only be determined through a time-consuming and costly process of research and testing.

3.72 Importantly, the defences of acquisition from public sources, reverse engineering and independent development only apply to situations where such acts were actually used by the defendant to acquire the trade secret information. The fact that such processes 'could have' been used is not proof of the absence of misappropriation, but it may be proof that the information is readily ascertainable and, therefore, not a trade secret.

D. Statute of limitations

3.73 The UTSA includes a statute of limitations (section 6) that requires trade secret misappropriation claims to be brought 'within 3 years after the misappropriation is discovered or by the exercise of reasonable diligence should have been discovered'. The commentary to the UTSA specifically states that trade secret misappropriation is not a continuing wrong, but should be measured from the date of the alleged wrongdoing of each defendant. Although most states that have adopted the UTSA have enacted its statute of limitations, some states have modified the number of years or have chosen to rely upon the general statutes of limitations applicable in those states.

E. Preclusion of other laws

3.74 One of the problems that the UTSA sought to solve concerns the existence of a variety of common law theories of recovery for the alleged misappropriation of business information, coupled with the inconsistent (and sometimes overly broad) meanings of trade secrets and misappropriation under those theories.[27] Consistent with the notion that not all business information is deserving of protection under the law, section 7 of the UTSA provides that all common law tort claims for misappropriation of information alleged to be a trade secret are precluded by the UTSA. In states that interpret section 7 in a manner that is consistent with its purpose (and most do), this means that the only causes of

27 See Charles Tait Graves, 'Trade Secrecy and Common Law Confidentiality: the Problem of Multiple Regimes' in Rochelle C. Dreyfuss and Katherine J. Strandburg (eds), *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research* (2011), p. 537.

action a putative trade secret owner can bring related to the alleged misappropriation of business information are (1) a claim under the UTSA and, where applicable based upon the facts, (2) breach of contract, and (3) breach of fiduciary duty claims.

F. Other defences

3.75 The UTSA does not include any explicit public interest defences as are contained in the proposed EU Trade Secret Directive, discussed in Appendix 1. However, the common law origins of trade secret law in the United States should allow such arguments to be made in the right case, such as where there is a strong public interest in learning information that is relevant to public health and the environment.[28]

3.76 The UTSA does not preclude the assertion of any legal or equitable defences that might exist under common law or by statute. Thus, various equitable defences, such as laches and acquiescence, have been asserted in US trade secret cases. In cases where the plaintiff has sought an injunction that would prevent the defendant from disclosing (and therefore speaking about) the trade secrets, a defence based upon the free speech principles of the First Amendment to the US Constitution have also been asserted.[29] Arguments have also been made in some cases that the plaintiff's over-assertions of trade secret rights is anti-competitive or inequitable.[30]

VI. AVAILABILITY OF REMEDIES, INCLUDING THE MEASURE OF DAMAGES

3.77 Because trade secret law first developed in the United States through the common law process of law, the remedies for trade secret misappropriation that traditionally applied mirrored both the scope and limits of remedies available at common law for equitable, tort and contract claims. The significance of the UTSA is that it clarified and broadened the availability of remedies to include potential remedies that were not typically available at common law, including a broader measure of damages and the availability of reasonable royalties, attorney's fees and punitive damages in some situations. The following provides a

28 See e.g., the common law of the United Kingdom, discussed in Chapter 7.

29 See e.g., *Ford Motor Co.* v. *Lane*, 67 F.Supp.2d 745 (E.D. Mich. 1999). See also, Pamela Samuelson, 'First Amendment Defenses in Trade Secrecy Cases' in Rochelle C. Dreyfuss and Katherine J. Strandburg (eds), *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research* (2011), p. 537.

30 Harry First, 'Trade Secrets and Antitrust Law' in Rochelle C. Dreyfuss and Katherine J. Strandburg (eds), *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research* (2011), p. 537.

brief summary of the civil remedies that are available under the UTSA. For more detailed information, see Chapter 6.

A. Permanent injunctive relief

3.78 Section 2 of the UTSA spells out the circumstances where permanent injunctive relief may be granted (although as explained below, such relief should end when the trade secrets cease to exist and, therefore, is not really 'permanent'). Section 2 explicitly states that 'actual or threatened misappropriation may be enjoined'.

3.79 Although not included in the language of section 2 itself, it is generally recognized that traditional principles of equity apply in the United States to determine if and when an injunction will be issued, including the classic requirements under US law of irreparable harm and the inadequacy of legal remedies. In this regard, there is a question under US law whether irreparable harm should be presumed once a finding of trade secret misappropriation is made or whether the plaintiff in a trade secret case must address the well-established equitable factors for the grant of injunctive relief. As a practical matter, resolution of this issue depends upon whether the alleged trade secrets continue to exist at the time a permanent injunction would be ordered.

3.80 At the time the UTSA was drafted, there was a conflict of authority among some courts concerning the proper length of injunctive relief. Some courts believed that perpetual injunctions were appropriate to punish trade secret misappropriators even if the underlying trade secrets subsequently ceased to exist due to no fault of the enjoined party. Other courts believed that given the fleeting nature of trade secrets, injunctive relief should only last for as long as the subject information remained a trade secret. Section 2(a) of the UTSA explicitly adopts the position that injunctions should end when the trade secrets cease to exist, with the proviso that an injunction may be 'continued for an additional reasonable period of time in order to eliminate commercial advantage that would be derived from the misappropriation'. This period of time is what is commonly referred to as the 'lead-time' (or head start) advantage and is generally the period of time that the misappropriator had access to the trade secrets before they became generally available.

B. Preliminary injunctive relief

3.81 No provision of the UTSA specifically addresses the availability of preliminary relief, other than the general provision on injunctive relief which provides that

'actual or threatened misappropriation may be enjoined'. Based upon well-established principles of equity that are followed by both the state and federal courts in the United States, however, procedures and standards exist for the grant of preliminary relief. Generally, a written request in the form of a motion for preliminary relief must be filed with the court and served on the defendant(s).[31] Then, a number of equitable factors must be considered.

3.82 As is the case with permanent injunctions, discussed above, preliminary injunctions can be extinguished once it is demonstrated that the trade secrets covered under the injunction have ceased to exist. This is ordinarily accomplished by the enjoined party filing a motion to extinguish the injunction with the appropriate court.

C. Compensatory damages

3.83 The damages provisions of the UTSA are set forth in section 3 and are significant because they broaden the available measures of damages beyond the traditional expectation damages of contact law or the lost profits measure of damages generally applicable to business torts. Section 3(a) of the UTSA provides that '[d]amages can include both actual loss caused by misappropriation and the unjust enrichment caused by misappropriation that is not taken into account in computing actual loss'.

D. Reasonable royalties

3.84 In addition to compensatory damages measured by actual loss to the plaintiff or unjust enrichment to the defendant, section 3(a) of the UTSA further states that 'in lieu of any other measure of damages', damages may be measured by a reasonable royalty. In practice, the reasonable royalty measure of damages is usually claimed in rare situations where the plaintiff has no lost profits because it is not currently in business and where the defendant has no measurable unjust enrichment.

3.85 An interesting and unique provision of section 2 of the UTSA allows courts to grant a reasonable royalty in lieu of an injunction in 'exceptional circumstances'. Exceptional circumstances 'include, but are not limited to, a material and prejudicial change of position prior to acquiring knowledge or reason to know of misappropriation that renders a prohibitive injunction inequitable'.[32] This would apply to the 'accidental' or 'innocent' acquirer situations (discussed

31 See e.g., Fed. R Civ. P r. 65(a).
32 UTSA, s. 2(b).

above) where a third party did not know or have reason to know of the trade secret misappropriation upon first acquiring the trade secrets.

3.86 The exception allowing for reasonable royalties instead of an injunction in exceptional circumstances was intended to ameliorate the change that the UTSA made to common law which, traditionally, did not impose liability on innocent acquirers.[33] According to the drafting history of the UTSA, the exception is also meant to apply in circumstances where 'an overriding public interest' requires the denial of a prohibitory injunction. The case cited in support of this proposition involved a misappropriator that was using the plaintiff's trade secrets to supply critical aircraft weapons control systems to the military during the war in Vietnam.[34] At least one court has noted that 'society's general interest in fostering competition' does not 'rise to the level of an overriding public interest' such that injunctive relief for misappropriation may be denied.[35]

E. Exemplary damages

3.87 Exemplary (or punitive) damages are provided for in section 3(b) of the UTSA but they are limited to a maximum of two times any award of actual damages. Additionally, exemplary damages are only available in cases where 'willful and malicious misappropriation' is found, which is interpreted to mean a state of mind and degree of wrongfulness that is more egregious than trade secret misappropriation itself. Generally, a motive to compete (even aggressively) is not enough to constitute willful and malicious behaviour.[36]

F. Attorney's fees

3.88 Pursuant to the so-called American rule, attorney's fees are not generally awarded to the prevailing party in civil litigation matters in the United States. However, this rule can be modified by contract and, as is discussed in Chapters 4 and 5, an attorney's fees clause may be included in the various agreements that are entered into between trade secret owners and their employees and vendors. With respect to any trade secret misappropriation claims, however, section 4 of the UTSA allows for the award of attorney's fees only in limited situations.

---

33 *Ibid*. s. 2 comment.

34 *Republic Aviation Corp.* v. *Schenk*, 152 USPQ 830 (NY Sup. Ct 1967).

35 *Progressive Products, Inc.* v. *Swartz*, 205 P.3d 766, 778 (Kan. Ct App. 2009).

36 See *Roton Barrier, Inc.* v. *Stanley Works*, 79 F.3d 1112, 1120 (Fed. Cir. 1996).

3.89 Pursuant to section 4 of the UTSA, if the plaintiff in a trade secret misappropriation case prevails, she may be awarded reimbursement of attorney's fees only if wilful and malicious misappropriation is proven. If the defendant prevails (either on the entire case or on a motion to terminate an injunction), attorney's fees may be awarded to the defendant upon a showing that the misappropriation claim or the opposition to the motion to terminate the injunction were brought in bad faith. The provision allowing defendants to recover attorney's fees was specifically designed to deter the filing of specious trade secret misappropriation claims, although (as is discussed in Appendix 1) it is arguably not as broad as comparable provisions in the proposed EU Trade Secret Directive.

3.90 Where attorney's fees are granted, it is within the sound discretion of the courts to determine the amount of any award and whether the hourly rate charged and the hours incurred on a case are reasonable.

VII. PROTECTING TRADE SECRETS DURING LITIGATION

3.91 A risk that all trade secret owners face when initiating trade secret litigation is the potential loss of trade secrecy as a result of the litigation process itself, including any administrative or criminal proceedings. For this reason, a major priority of trade secret harmonization efforts is to require countries to provide means for trade secrets to be protected during litigation.

3.92 In the United States, protective orders that limit the use and disclosure of trade secrets and other business information are generally available upon a proper showing in both state and federal courts. The UTSA specifically requires that they will be available in trade secret cases.

3.93 Section 5 of the UTSA states that 'a court shall preserve the secrecy of alleged trade secrets by reasonable means'. This may include the issuance of a protective order, *in camera* hearings and presentations of evidence, and the sealing of court records. In practice, it typically includes requiring all persons who may be exposed to trade secrets (except the jury and the judge) to specifically agree to maintain the alleged trade secrets in confidentiality.

3.94 The ability to protect trade secrets during trial in the United States is more problematic than the process of protecting trade secrets during the pleading and discovery phases of a case. This is due to the strong public policy in the United States that favours open and transparent courtroom proceedings. The same goes for the sealing of court records after a trial. If it has been proven that

specific information is a trade secret, then the sealing of court files to maintain the secrecy of that information (at least until such time as it otherwise becomes public) is appropriate. However, broad orders to protect all proceedings related to a trade secret case are disfavoured.

3.95 The desire of trade secret owners to protect the secrecy of their trade secrets during litigation must be balanced against the need of defendants to understand the claims being made against them. This is particularly true in criminal trade secret prosecutions where principles of due process require such notice. Thus, while a trade secret owner often objects to having to disclose the specifics of its trade secrets too soon or too often, typically the details of the trade secrets must be disclosed sufficiently before trial so that the defendant can conduct a prior art search and otherwise fashion a defence. In the United States, the failure of a plaintiff to adequately and timely identify its alleged trade secrets may result in a dismissal of plaintiff's claims or a judgment in favour of the defendant. Appropriately worded protective orders will preserve the relative secrecy of the trade secrets while still allowing the defendant to understand the details of those secrets and obtain a fair trial.

VIII. PUBLIC POLICY LIMITS ON SCOPE AND APPLICATION OF TRADE SECRET PROTECTION

3.96 Although not framed or labelled as such in the UTSA, the foregoing requirements and details of trade secret law serve as important limitations on the scope and application of trade secret law and reflect a number of countervailing public policy concerns that should be taken into account when interpreting and applying US trade secret law.

3.97 First, there is the public policy of access to information and knowledge diffusion that is reflected in the fact that trade secret law cannot protect information that is generally known or readily ascertainable. Based upon a series of US Supreme Court cases, it is clear that the maintenance and sharing of a rich public domain is an important policy of the United States.[37]

3.98 Second, another important policy that underlies US trade secret law (and more broadly all intellectual property laws) is the policy of free competition. As summarized in commentary to the first section of the *Restatement (Third) of Unfair Competition*, '[t]he freedom to engage in business and to compete for the patronage of prospective customers is a fundamental premise of the free

37 See e.g., *Bonito Boats, Inc.*, 489 US 141, n. 11 above, and cases cited therein.

enterprise system'. Based upon the foregoing, it is generally recognized that free competition is the rule and intellectual property (including trade secret) protection is the exception.

3.99 Applied correctly, trade secret law will not hamper free competition but instead will only restrict behaviour that crosses the line and becomes 'unfair competition'. The details and requirements of the UTSA help to define when this line is crossed. If legitimate trade secrets exist and have been wrongfully acquired, disclosed or used with the requisite state of mind, the line has been crossed. Absent those facts, there is generally nothing wrong with companies collecting information about their competitors in an effort to be more competitive, unless they engage in activities that are otherwise tortious or illegal.

3.100 Third, although the public policy of the United States that favours employee mobility does not find direct expression in the UTSA, it can be found in the common law and statutes of the states, including principles of employment law. Generally, neither trade secret law nor employment law should be applied in a manner that unduly restricts employees in their ability to better themselves and find better places of employment.

3.101 As is explained in more detail in Chapter 5, because of the policy that favours employee mobility, restrictive covenants and non-compete agreements that are designed to limit employee mobility are carefully scrutinized by US courts for reasonableness and will not be enforced unless they are limited in scope and time. In some states, these agreements are *void ab initio*, except in very limited situations.

3.102 Fourth, while the 50 US states are generally free to adopt laws to regulate activity within their borders, when the US Congress exercises its limited powers to adopt federal laws, sometimes a conflict between state and federal law arises that must be resolved. Pursuant to principles of federal pre-emption, US federal law can trump state law and make the state law unenforceable in some situations. With respect to state trade secret laws, a conflict between state and federal laws may arise if the state law is written or applied in such a manner that it conflicts with the patent and copyright policies of the United States.

3.103 In *Kewanee* v. *Bicron Oil Co.*, the US Supreme Court ruled that the trade secret law as applied at the time by the State of Ohio was not pre-empted by US patent law, but a careful reading of that case indicates that the scope of trade secret protection in Ohio was carefully circumscribed. Thus, whether the ruling of *Kewanee* is applicable to the laws of other states (and the laws of Ohio as they currently exist and are applied) is an open question. Importantly, the principles

of *Kewanee* and the potential conflicts between state trade secret principles and US patent and copyright laws serve to define the outer boundaries of state trade secret law in the United States.

4

TRADE SECRETS AND BUSINESS TO BUSINESS RELATIONSHIPS

I. INTRODUCTION

4.01 In this age of global commerce and the transnational operation of companies large and small, the relationships between companies and their business partners has taken on greater importance from a trade secret perspective. This is because unless a company prefers to keep most of its business operations in-house, it not only has to worry about its own trade secret practices but also the trade secret practices of all companies with which it does business. While this generally requires trade secret owners to establish obligations of confidentiality with every company that is given access to its trade secrets (including, possibly, all companies in its supply chain), for offshore relationships it also requires companies to understand how those obligations of confidentiality are formed and are likely to be enforced in other countries.

4.02 As discussed in Chapters 2 and 3, with respect to both Article 39 of the TRIPS Agreement and the Uniform Trade Secrets Act (UTSA), the breach of a duty of confidentiality is one of two predicates to liability for trade secret misappropriation, the other one being acquisition by improper means. The existence of a duty of confidentiality is also an important factor in determining whether a trade secret owner engaged in reasonable efforts to maintain the secrecy of its information. Thus, it is essential that trade secret owners establish an obligation of confidentiality with their business partners before sharing any trade secret information.

4.03 Although the initial issue that arises with respect to trade secrets that are shared in a business to business relationship is whether the trade secret owner engaged in reasonable efforts to maintain the secrecy of its information, practically speaking, no trade secret owner wants to be put in the position of having to explain and defend its trade secret protection efforts. The better outcome is to prevent trade secrets from being misappropriated in the first instance and this can only be accomplished by instituting a carefully designed trade secret protection strategy that looks beyond the act of exacting a promise of confidentiality to consider how trade secret information will actually be used and distributed.

4.04 In practice, a company's trade secret protection strategy will be part of an overall information and knowledge management system which, typically, will have to deal with information coming from a variety of sources. Depending upon the nature of a company's business, this can be a rather complicated process involving not only a company's own trade secrets and proprietary information, but information that is licensed from others and information created by employees. It may also involve the need to comply with laws that are ancillary to trade secret law, including data privacy laws, government contract requirements and export restrictions. While the failure of a company to institute adequate measures to protect its own trade secrets can result in the loss of trade secrecy, the failure of a company to protect the trade secrets of another and to comply with applicable law can expose it to lawsuits and, in some cases, criminal prosecution.

4.05 Further complicating the analysis of trade secret protection in business to business relationships is the fact that businesses (like individuals) need information and knowledge to conduct their day-to-day operations, learn from their mistakes and improve their processes and performance. Although in theory it might be possible to physically secure much of the information that is used by a business, in practice a business might benefit more from the free exchange of ideas than from an aggressive information protection strategy. Thus, no trade secret protection strategy should be devised without considering how information must flow within and without a business. For some businesses in some industries, an open innovation model may be more appropriate while in others strict policies are needed to keep track of and carefully guard information which must be kept secret.[1]

1 See William H. Honaker, 'IP and the Open Innovation Model' in Sharon K. Sandeen (ed.), *Intellectual Property Deskbook for the Business Lawyer: A Transactions-based Guide to Intellectual Property Law* (2013), p. 259.

4.06 With the amount of information that flows in and out of a business, some of it requiring confidential handling and some of it available to be used freely, it can be extremely difficult for the executives of a company, let alone its employees, to keep track of which body of information should be treated as trade secret information. Many companies (and their attorneys) are inclined to want to protect all business information as trade secrets and restrict its use, but this is not realistic given the need for information in the operation of a business. The better practice is to identify the various types and sources of information that a business possesses and uses, and categorize that information according to the levels of protection that is needed for each, with trade secret information typically requiring greater protection than other types of business information.

4.07 Looking through the lens of US trade secret law, this chapter discusses strategies for effectively gathering, sharing and protecting important business information. It begins with the important issue of how to establish binding and enforceable confidentiality agreements with other businesses. While the applicable law also applies to relationships with employees, as discussed in Chapter 5, it is usually more difficult to establish implied duties of confidentiality in business to business relationships because of the arm's length nature of those relationships. Thus, as discussed below, express written agreements in the form of confidentiality agreements and license agreements play a big role in the protection of trade secrets that are shared among businesses.

4.08 In addition to explaining how duties of confidentiality with other businesses can be established, this chapter examines several other issues related to the gathering, sharing and protection of business information, including: (1) how to effectively manage and protect trade secret and other proprietary information that is received from others; (2) how to engage in 'proper' information gathering and competitive intelligence; and (3) how to guard against lawsuits by so-called 'idea men and women'. The latter issue typically arises when individual inventors or creators submit unsolicited information to companies. Strategies for protecting trade secrets and other proprietary information in dealings with governmental officials are discussed in Chapter 7.

II. CONFIDENTIALITY IN BUSINESS RELATIONSHIPS

4.09 Companies often need to share information with entities and persons outside of the company, such as with subcontractors, vendors, and joint development and other business partners. However, the voluntary sharing of information ordinarily results in a loss of trade secret protection for the shared information. This is due to the third party doctrine of trade secret law that is discussed in Chapter

3 and is similar to concepts of waiver under applicable patent and privacy laws and under Fourth Amendment jurisprudence in the United States.[2] The phenomenon has been labelled by economists as 'Arrow's information paradox' or the 'double trust dilemma of innovation'.[3]

4.10 One of the recognized purposes of trade secret law is to solve Arrow's information paradox by facilitating the necessary sharing of information among businesses in a manner that does not result in the loss of trade secrecy. In the United States and some other countries, this is accomplished through application of the 'relative secrecy doctrine'. Pursuant to the relative secrecy doctrine, trade secrets are not destroyed if they are only shared in the context of a confidential relationship. What constitutes relative secrecy, however, is a fluid concept that is likely to differ among countries, not only because each country may have differing standards of relative secrecy and confidential relationships, but because application of the concept requires a very fact specific analysis and often depends upon the equities of the situation.

4.11 The UTSA does not use the phrase 'duty of confidentiality' and does not define the scope and meaning of a duty of confidentiality in either the text of the UTSA or the commentary. However, it does define misappropriation to include disclosing or using a trade secret of another with knowledge or reason to know that it was acquired 'under circumstances giving rise to a duty to maintain its secrecy'.[4] Accordingly, the meaning of this duty is usually determined by the common law of each individual state and can prove to be a very flexible requirement.

4.12 The best way to ensure that trade secrets that are shared with another business are kept relatively secret is for the trade secret owner to enter into an express written agreement of confidentiality with the recipient of the trade secrets before any sharing of information occurs. Such an agreement can take several forms. It may take the form of a separately negotiated document labelled 'confidentiality agreement' or 'non-disclosure agreement' or it may be expressed as one or more clauses in a broader agreement, such as a license agreement. The key features of confidentiality agreements are discussed next, followed by a discussion of implied duties of confidentiality. License agreements are discussed thereafter.

---

2 See Sharon K. Sandeen, 'Lost in the Cloud: Information Flows and the Implications of Cloud Computing for Trade Secret Protection' (2014) 19 *Va. J L and Tech.* 1.

3 See Kenneth J. Arrow, 'The Value of Demand for Information' in C.B. McGuire and R. Radner (eds), *Decision and Organization* (2nd edn 1987); Robert D. Cooter and Hans-Bernd Schäfer, *Solomon's Knot: How Law Can End the Poverty of Nations* (2012), ch. 3.

4 Uniform Trade Secrets Act, s. 1(2)(ii)(B)(II) (amended 1985).

A. Confidentiality agreements

4.13 The term 'license agreement', discussed below, is the label that is typically used for agreements that allow the recipient of information to use information over an extended period of time. In contrast, the term 'confidentiality (or non-disclosure) agreement' is typically used in conjunction with one-time or infrequent business deals.

4.14 Regardless of the label that is used, typically, confidentiality obligations (or clauses) specify: (1) the parties to the agreement; (2) the information to be protected; (3) the manner in which the information can be used; (4) an express promise of confidentiality; and (5) the length of the confidentiality obligation. More sophisticated and protective confidentiality agreements, and those that are sensitive to the reasonable efforts requirement of trade secrecy, will include detailed provisions concerning required security measures and limits upon who can access the information. In particular, it is important to consider whether and under what circumstances the subject information can be shown to third parties, for instance subsidiaries of the recipient or its outside counsel and experts. Additionally, such agreements will often require that all shared information be marked with prescribed legends such as 'confidential' or 'trade secret'.

4.15 If the contemplated business relationship requires the exchange of information by both (or all) parties, then the duty of confidentiality will usually be reciprocal. However, if one (or more) of the parties will only be giving and not receiving information, reciprocal obligations of confidentiality are not needed and should be avoided by licensors. Because of the general need for information flow within business enterprises, no business should voluntarily agree to restrictions on the free flow of information or to a duty of confidentiality that, even if factually superfluous, might expose it to a claim for breach of confidentiality or hamper its business operations.

4.16 Although principally designed to protect legitimate trade secrets, businesses will often use an express confidentiality agreement to expand the universe of protected information to 'proprietary and confidential' information, 'improvements' and 'know-how', often without defining those terms. This type of provision is protective of the recipient of information because it needs to be certain that it receives sufficient information to evaluate the business deal or to effectively utilize the trade secrets. It is also protective of the information owner because it wants to protect all of the shared information and not just the information that meets the strict legal definition of a trade secret. Nonetheless, it is important to identify the information that is claimed to be a trade secret. Of course, the trade secrets themselves should not be revealed in the agreement,

but they should be described sufficiently so that the parties can identify them and distinguish them from other shared information.

4.17 As with most contractual agreements, it is typical for confidentiality agreements (or agreements with confidentiality clauses) to terminate after a period of years. However, this does not make sense with respect to an obligation of confidentiality if the trade secret and confidential status of the shared information is expected to last longer than the term of the agreement. Thus, it is not uncommon for confidentiality agreements to extend for a longer period of time than the other requirements of an agreement. With respect to trade secrets, a duty of confidentiality should be written to apply for as long as the trade secret status of the information subsists. It is also advisable to require the return or destruction of all shared information (particularly trade secrets) upon the revocation or termination of the confidentiality agreement.

4.18 From the perspective of the recipient of trade secrets, it is generally advisable that any confidentiality agreement include a 'carve-out clause' which specifically and clearly states that the duty of confidentiality does not apply to information that: (1) is generally known publicly and among people skilled in the art; (2) is readily ascertainable from public sources, including publications and products that are on sale or otherwise distributed to the public; (3) is within the general skill and knowledge of the executives, employees and agents of the recipients of the information; or (4) was reverse engineered or independently developed by the party against whom the obligation of confidentiality is being asserted (unless enforceable restrictions are placed upon such activities as discussed below). The carve-out clause should also make it clear that it applies to the foregoing categories of information whether they existed before the effective date of the confidentiality agreement or came to be after such date, provided that the disclosures were not in breach of the confidentiality agreement.

4.19 Sometimes confidentiality agreements are used to further restrict the behaviour of one or more parties, for instance, by prohibiting the parties from engaging in reverse engineering and independent development activities. Whether these provisions are enforceable or can serve as a basis for a successful trade secret misappropriation claim are typically issues to be resolved during a trial. A key issue is whether principles of freedom of contract should apply or whether reverse engineering and independent development are in the nature of rights that cannot be waived. In either case, care should be taken to ensure that the extension of a confidentiality agreement beyond the protection of legitimate trade secrets is not viewed as an improper restraint of trade or otherwise anticompetitive.

4.20 It is also not uncommon for confidentiality agreements to include clauses that try to anticipate the remedies the parties will need in the event of a breach of the agreement. As detailed in Chapters 3 and 6, the remedies for trade secret misappropriation under the UTSA can include both injunctive relief and monetary damages, but typically the trade secret owner will want to act quickly to obtain a temporary restraining order or preliminary injunction in an effort to prevent a loss of trade secrecy. The trade secret owner may be able to enhance its ability to obtain a prompt injunction by including a clause in the confidentiality agreement whereby the recipient of information agrees that injunctive relief is proper and, further, that any security requirement is waived. A liquidated damages provision may also be included that applies in the event of the disclosure of the information. However, such a clause may be viewed as being inconsistent with an argument (often needed to obtain injunctive relief in the United States) that the trade secret owner suffered irreparable harm.

4.21 As with contracts generally, confidentiality agreements can also be used to anticipate and solve other issues that might arise in future litigation, including the applicable choice of law and issues of personal jurisdiction and venue. Such provisions are particularly helpful in relationships involving multiple parties located in different jurisdictions and in situations where one or more parties may change the location of their principal place of business. Ideally, the trade secret holder will use such provisions to make its ability to enforce the confidentiality agreement easier by, for instance, specifying the jurisdiction and the law that it favours. Finally, confidentiality agreements often include an attorney's fees provision that requires the prevailing party to be reimbursed for the attorney's fees and costs it incurred in bringing an action to enforce the agreement.

4.22 Keep in mind that the enforcement of confidentiality agreements ultimately depends upon the other party's willingness to voluntarily comply with both the agreement and any enforcement order or judgment that might be rendered with respect to such agreement. If court intervention is needed to enforce a judgment or court order, the location of the enforcing court will often dictate the outcome. For example, just because a court order is obtained in the United States does not mean that it will be enforced in China, and *vice versa*. Thus, careful thought must be given in advance to whether the other party to a confidentiality agreement will voluntarily comply with any court order and, if not, how the order will be enforced and by whom.

4.23 In light of potential enforcement issues, particularly with respect to companies that are located in another country, consideration should be given to whether the confidentiality agreement ought to include an arbitration clause and, if so,

where and before which arbitral forum, disputes will be arbitrated. Given the likely need for quick injunctive relief to protect trade secrets, the ability of the arbitral forum to grant timely injunctive relief should be determined and specified as necessary.

4.24 Pursuant to the general principles of contract law and the associated principle of freedom of contract, businesses are usually free to decide the terms of their contracts with other businesses and, absent some overriding public policy, those contracts are likely to be enforced. However, consideration should always be given to whether particular terms of a contract may be unenforceable in a given country and, if so, whether the entire agreement will be invalidated or just the unenforceable part. In this regard, some countries may require that certain types of contracts be filed with government officials for review. Insights regarding these issues are provided in Chapters 9 and 10 with respect to the countries that are discussed therein.

4.25 Generally, because confidentiality agreements are restraints of trade, they are apt to be scrutinized carefully by courts as well as by antitrust and competition officials to determine if they are reasonable. However, unlike confidentiality agreements that are used in the employment setting where a principal concern is employee mobility (discussed in Chapter 5), the focus of the inquiry with respect to confidentiality agreements in arm's length business dealings is likely to be much narrower. Clauses that might attract particular scrutiny are those that purport to prevent the use of public information and that restrict independent development and reverse engineering.[5]

B. Implied duties of confidentiality

4.26 In the absence of an express written obligation of confidentiality, companies that need to prove that their trade secrets were kept relatively secret at the time they were shared with another company will face the unenviable task of proving the existence of either an express oral or an implied agreement of confidentiality. Generally, this is governed by the law of contracts of each country or by laws and legal principles that otherwise define duties of confidence. For instance, the United Kingdom has a well-developed body of law concerning common law duties of confidence, as discussed in Chapter 9.

4.27 In the United States, the most obvious relationship giving rise to a duty of confidentiality is a trust or fiduciary relationship, such as the attorney/client

5 See below for a discussion of these issues in the licensing context.

relationship.[6] Absent a trust or fiduciary relationship, whether a particular business relationship gives rise to an implied duty of confidentiality often requires application of the law governing implied-in-fact and implied-at-law contracts.[7] Generally, when a relationship involves business entities of similar sophistication and bargaining power, it can be difficult to establish an implied duty of confidentiality under US law.[8] Nonetheless, there are a variety of business relationships that may give rise to an implied duty of confidentiality depending on the circumstances.

4.28 Generally, whether or not an implied-at-law duty of confidentiality will be deemed to exist depends upon a number of factors, including: (1) the nature of the relationship; (2) the nature of the alleged trade secrets; (3) whether the person charged with misappropriation was aware of the existence of trade secrets and of the trade secret owner's desire for confidentiality; and (4) who is considered the owner of the trade secret.[9] Generally, the closer the relationship between a trade secret owner and another, the more likely it is that an implied-at-law duty of confidentiality will be found. However, even seemingly close relationships, like the employer/employee relationship, do not create a duty of confidentiality in all cases and under all circumstances.[10]

4.29 An issue that exists under US law and that might exist in other countries is whether the standards for forming confidential relationships are different, or less stringent, in trade secret cases than in other situations. While the UTSA does not define a duty of confidence, the *Restatement (Third) of Unfair Competition* provides that an implied duty of confidentiality arises when the circumstances justify the conclusion that the person receiving the information knew or had reason to know that the disclosure was intended to be in confidence and the trade secret owner was reasonable in inferring that the recipient of the information consented to an obligation of confidentiality.[11] While this standard may be viewed as a restatement of general principles of equity related to implied-at-law contracts, trade secret owners obviously prefer, and often assert, that it is a fairly easy standard to meet.

4.30 Based upon the foregoing, to determine whether an implied duty of confidentiality arose from the sharing of trade secrets requires an examination of: (1) the

6 See *Fischer* v. *Viacom Intern., Inc.*, 115 F.Supp.2d 535, 543 (D Md 2000); *Djowharzadeh* v. *City National Bank & Trust Co.*, 646 P.2d 616, 619 (Okla. Civ. App. 1982).

7 See *Reeves* v. *Alyeska Pipeline Services Co.*, 926 P.2d. 1130 (Alaska 1996).

8 See *Smith* v. *Snap-on Tools Corp.*, 833 F.2d 578 (5th Cir. 1987).

9 See *Zoecon Industries* v. *American Stockman Tag Co.*, 713 F.2d 1174, 1178 (5th Cir. 1983).

10 See e.g., *Shatterproof Glass Corp.* v. *Guardian Glass Co.*, 322 F.Supp. 854 (ED Mich. 1970).

11 *Restatement (Third) of Unfair Competition* (1995), s. 41(b).

circumstances surrounding the disclosure; (2) the recipient's state of mind; and (3) the reasonableness of the trade secret owner's actions. Two important circumstances are whether trade secrets existed and were shared with another and whether the recipient of the information was made aware of the expectation of confidentiality. Another important factor, particularly where equity plays a role, is the perceived wrongfulness of the behaviour.

4.31 The types of relationships where (based upon the specific facts of each case) an implied duty of confidentiality has been found in the United States include: a manufacturer and its suppliers;[12] a manufacturer and an independent contractor;[13] the seller of a business and a potential buyer;[14] a licensor and licensee;[15] an independent inventor and a potential manufacturer of his invention;[16] and where a trade secret owner provides a product for testing and evaluation.[17] A court in the United States even ruled that a duty of confidentiality may exist between joint owners of a trade secret.[18]

4.32 In practice, the line between an interaction that gives rise to an implied duty of confidentiality and those that do not can be very fine and will obviously differ from country to country. In the United States, where the line is drawn often depends upon whether the disclosure of information was solicited or unsolicited. Although it may seem unfair for a business to use information that it received from another without paying for it, the business that receives unsolicited information does not want to be subjected to trade secret misappropriation claims merely because they listened to someone's pitch. Courts in the United States have held that the mere act of disclosing information to a third party does not create a duty of confidentiality.[19] Among other reasons, disclosing what one believes to be a trade secret without alerting the recipient that it is a trade secret that must be protected fails to put the recipient on notice of the need for confidentiality.

4.33 Despite the foregoing, there is commentary in the *Restatement (First) of Torts* to the effect that the act of sharing information, when coupled with notice that it is a trade secret, can be enough to create a duty of confidentiality in the United

12 See *Flotec, Inc.* v. *S. Research, Inc.*, 16 F.Supp.2d 992, 998 (SD Ind. 1998).
13 See *Hicklin Engineering, LC* v. *Bartell*, 439 F.3d 346 (7th Cir. 2006).
14 See *Smith* v. *Dravo Corp.*, 203 F.2d 369 (7th Cir. 1953); *Phillips* v. *Frey*, 20 F.3d 623 (5th Cir. 1994).
15 See *Hyde Corp.* v. *Huffines*, 314 SW 2d 763 (Tex. 1958).
16 See *Kamin* v. *Kuhnau*, 374 P.2d 912 (Or. 1962).
17 See *Mineral Deposits Ltd* v. *Zigan*, 773 P.2d 606, 608 (Colo. App. 1988); *Morton* v. *Rank America, Inc.*, 812 F.Supp. 1062, 1074 (CD Cal. 1993).
18 See *Morton* v. *Rank America, Inc.*, 812 F.Supp. 1062, 1074 (CD Cal. 1993).
19 See *Smith,* 833 F.2d, n. 14 above, at 579–80 ('[W]hen parties are dealing at arm's length, one party's disclosure of an alleged trade secret to another does not automatically create a confidential relationship').

States.[20] The cases that apply this broad conception of an implied duty of confidentiality in trade secret cases often involve information that was expressly solicited (or enthusiastically welcomed) by the alleged misappropriator.[21] The circumstances surrounding the disclosures and the positions of power between the parties are additional factors that can lead to a finding of an implied duty of confidentiality.[22]

4.34 When determining the existence of an implied duty of confidentiality, the nature of the information to be protected (whether it rises to the level of a trade secret) can be critical because it determines the available causes of action and remedies. Thus, in the United States it is theoretically possible that someone could breach a duty of confidentiality but not be subjected to a successful claim for relief. This could happen where: (1) the information is not a trade secret and, therefore, no trade secret claim can be brought successfully; (2) the duty of confidentiality is not a contractual duty, so no breach of contract claim can be asserted successfully; and (3) where the particular jurisdiction interprets section 7 of the UTSA broadly to preclude tort claims not based upon the misappropriation of a trade secret.[23]

III. TRADE SECRET LICENSE AGREEMENTS

4.35 In addition to confidentiality agreements, another way that businesses share trade secrets and other business information is in the form of license agreements.[24] License agreements are different from confidentiality agreements in a couple of respects. First, where as confidentiality agreements between businesses are frequently one-off agreements associated with specific negotiations, a license agreement often represents the development of a long-term synergistic relationship. As such, trust plays an important role not only in the protection of the licensed business information, but in the furtherance of the business relationship. Second, a license agreement typically includes compensation for the use of the licensed information. Nonetheless, many of the issues that were discussed with respect to confidentiality agreements, above, also apply to license agreements, including issues with respect to standard contract provisions.

---

20 See *Phillips*, 20 F.3d, n. 14 above, at 632 ('[N]o particular form of notice is needed; the question raised is whether the recipient of the information knew or should have known that the information was a trade secret and the disclosure was made in confidence'), citing *Restatement of Torts* (1939), s. 757 comment j.

21 See e.g., *Moore* v. *Marty Gilman, Inc.*, 965 F.Supp. 203, 215 (D Mass. 1997).

22 See *Learning Curve Toys*, *Inc.* v. *PlayWood Toys, Inc.*, 342 F.3d 714, 725–6 (7th Cir. 2003).

23 See Chapter 3.

24 See Christopher A. Sloan and William K. Norton, 'Licensing Intellectual Property' in Sharon K. Sandeen (ed.), *Intellectual Property Deskbook for the Business Lawyer: A Transactions-based Guide to Intellectual Property Law* (2013), p. 89.

4.36 Trade secrets can be licensed formally by written agreement and informally where the circumstances suggest that the licensee has impliedly agreed to certain duties to the trade secret owner. However, the most advisable situation is to enter into a written license agreement which makes clear the appropriate terms relating to such issues as confidentiality, royalties and duration of the agreement.

4.37 Trade secret licensing agreements can be simple or highly complex and can be stand-alone agreements or a part of a larger agreement. At a minimum they usually specify: (1) the parties to the agreement; (2) the information that is being licensed; (3) the manner in which the licensed information can be used; (4) the applicable obligations of confidentiality; (5) the duration, revocability and termination of the licence; and (6) the compensation to be paid for the licensed information. It is not uncommon for such agreements also to include representations and warranties whereby the licensor represents that it owns the licensed information and that such information does not infringe the rights of others.

4.38 As noted in the discussion of express confidentiality agreements, above, the identification of the parties and the information being licensed can be tricky. The licensee needs to make sure that the right people are given access to the licensed information so that it can be used as intended. The licensor, on the other hand, wants to restrict the distribution of the information so that there is less risk of disclosure. Some license agreements limit the disclosure of trade secrets to specific individuals within the licensee company or to specific units of the licensee and typically prohibit the sublicensing of the licensed information. However, if the licensee operates multinationally, a listing of related or subsidiary companies that operate in the various countries may be needed to effectuate a binding agreement against those parties. Also, consideration should be given to whether subcontractors of the licensee need access to the information and, if so, how they will be bound to a duty of confidentiality.

4.39 With respect to the identification of the licensed information, it must be broad enough to cover what the licensee needs to utilize the information, but not so broad that it exposes unneeded trade secrets to possible disclosure. This is particularly true with respect to information that must be handled confidentially. If such information is defined too broadly, then the licensee is unnecessarily exposed to potential liability for breach of confidentiality; if it is defined too narrowly, then there is a risk that trade secrets will be lost. An appropriate carve-out clause, as discussed above with respect to confidentiality agreements, can often be used to find the optimum balance between these two risks.

4.40 As noted previously, typically, the description of the licensed information will include information that is in addition to the trade secrets themselves, such as 'confidential' and 'proprietary' information and 'know-how' related to a specified type of technology or business process. This is done so that the licensee can be certain that it gets all the information it needs to utilize the licensed information and in order to circumvent any disputes about which part of the licensed information actually constitutes trade secret information. Of course, understanding which part of the licensed information is likely to constitute trade secrets and which is not, relates to the value of the licensed information and should be reflected in the compensation to be paid.

4.41 From a trade secret perspective the most important parts of a license agreement (and a confidentiality agreement, discussed above) are the provisions that specify how and where the trade secrets can be used and how they must be protected and stored. Ordinarily, the licensor of the licensed information continues to maintain ownership of the information but permits the licensee to access or use it, subject to certain conditions. If the owner grants an exclusive license to another company it essentially agrees that the licensee will be the only one (including the trade secret owner) that will be permitted to use the information within the scope of the license rights. In the more commonly utilized non-exclusive license, the licensee obtains the right to use the licensed information with permission from the owner but recognizes that others may also receive a similar licence and that the licensor has a right to use the licensed information for its own purposes.

4.42 Typically, the licensor-owner retains all rights in the licensed information that are not specifically granted to the licensee, including any applicable patents or copyrights. Thus, if a licensee exceeds the scope of the rights granted, it may be subject to liability for trade secret misappropriation in addition to a possible breach of contract claim. It is therefore very important for a licensee to anticipate and properly describe all of the potential uses of the licensed information that it needs. It is also important for a licensee to educate its employees about the scope of the license grant and to make sure that they do not use the information in a manner that is beyond the scope of the license.

4.43 Licensees will readily agree to keep licensed information confidential but a confidentiality agreement alone should never suffice for the licensor. Instead, the licensor should insist that the licensee institute a trade secret protection plan that is at least as robust as its own, but even greater protection efforts may be needed in some situations and in some countries. The key features of such a plan should be spelled out in the license agreement itself or in an addendum thereto. Among other best practices, the licensee should be specifically required to

obtain confidentiality agreements from those employees that will be given access to the information, as further described in Chapter 5. It is also important for the licensor to institute processes to periodically monitor and assess the licensee's compliance with the required security measures.

4.44 As with confidentiality agreements, discussed above, sometimes license agreements are used to further restrict the behaviour of the licensee beyond what is required by law, for instance, by prohibiting reverse engineering and independent development. These provisions are controversial and may not be enforced because they conflict with the public policy that favours the free exchange of information and which allows for the 'proper' acquisition of information, discussed below. Thus, care should be taken to ensure that the extension of a license agreement beyond the protection of legitimate trade secrets is not viewed as anticompetitive or otherwise against public policy in the country where the enforcement of such agreement may be sought.

4.45 Another issue that arises in the licensing context (and that may or may not arise with respect to confidentiality agreements) concerns whether the license agreement and the rights to the licensed information can be assigned or transferred to another party, for instance, in the event that the original licensee is acquired by another company or declares bankruptcy. To avoid downstream disputes related to the possible acquisition of or bankruptcy of either the licensor or the licensee, it is best to anticipate such issues and address them in the license agreement by specifically stating whether the license agreement can be assigned or transferred. The same goes for any potential mergers and acquisitions involving the licensee of the information.

4.46 Careful thought should also be given to the duration of the license agreement and the circumstances, if any, under which the licensed rights can be revoked and the license agreement terminated. A common provision relates to the failure of the licensee to make required royalty payments, but the potential for non-compliance with the confidentiality provisions should also be addressed. This is where standard contract clauses with respect to liquidated damages, attorney's fees, jurisdiction, venue and arbitration may come into play, particularly with respect to companies located in another country.

4.47 As with confidentiality agreements, although a license agreement may terminate after a number of years, the confidentiality obligation should continue to exist for as long as the trade secrets and other confidential information remain secret. It is also advisable to require the licensee to collect and return (or destroy) all licensed information upon the revocation or termination of the license

agreement. Under the laws of some countries, the maximum length of license agreements may be prescribed and other limitations may apply.

4.48 While trade secret licenses permit the trade secret owner to share its information and reap licensing revenue, they also come with greater risk of inappropriate disclosure and misappropriation due to the simple fact that more people have access to the information. This is particularly true in situations where multiple non-exclusive licences are granted. In situations where the trade secret owner is particularly cautious and does not wish to risk disclosure of its trade secrets (even under terms of a confidentiality agreement with a competitor or joint venture partner), it may choose to enter into an alternative arrangement whereby it provides technical services to the other entity rather than entering into a license agreement and actually disclosing its trade secrets.

4.49 All licensees of intellectual property rights assume some risk that the licensed rights may be declared invalid in the future, but this risk is particularly acute with respect to trade secrets because of the fleeting nature of such rights and the fact that trade secrecy can be lost due to no fault of the licensor or the licensee. This could happen, for instance, if a third party independently develops the same information or properly acquires it through reverse engineering and later discloses to the public. Because of this risk, it is generally advisable that trade secret license agreements include a termination clause in the event that the licensed information loses its trade secret status or otherwise ceases to be of value.

4.50 If a licensee is concerned about continued secrecy as a condition of entering into a license agreement, the agreement must be clear on that point, otherwise the licensee may be bound to the agreed upon royalty payments for the full length of the license agreement or, if no term is specified, for as long as the licensed information is used.[25] Courts will uphold properly worded contractual provisions that limit a licensee's payment obligations to a defined period of time or the useful life of the trade secrets.[26]

4.51 Another issue that arises in trade secret licensing situations concerns the possible misappropriation of the licensed information by third parties or employees of either the licensor or the licensee. Licensing agreements should specify whether the licensor or licensee (or both) can or must sue for trade secret misappropriation and which party (or parties) will bear the costs for such

25 See *Warner-Lambert Pharmaceutical Co.* v. *John J. Reynolds, Inc.*, 178 F.Supp. 655 (SDNY 1959).
26 *NOVA Chemicals, Inc.* v. *Sekisui Plastics Co.*, 579 F.3d 319, 326 (3rd Cir. 2009).

litigation. This might avoid standing problems if litigation becomes necessary and also helps ensure that the applicable trade secret rights will be enforced by someone.

4.52 Sometimes a trade secret license agreement will involve intellectual property rights in addition to trade secrets, most typically patent rights. Attorneys in such cases should be careful to understand and plan for the implications of these hybrid agreements. One practical limitation, for example, has to do with the different rules regarding the collection of royalties after the expiration or invalidation of a patent and a trade secret. While one may not collect royalties after a patent expires or is held invalid,[27] trade secrets are different. As discussed above, even after a trade secret is no longer secret it is possible that the owner-licensor may continue to collect royalty payments if the license agreement is not written to avoid this outcome.[28] Thus, counsel should consider separating out the patent and trade secret provisions regarding consideration, royalty payments and expiration terms or, ideally, prepare separate license agreements for each. The same goes for any licensed copyrights since the licensor of such rights has a statutorily prescribed termination right that may come into play in the future.[29]

4.53 A final issue to consider as a part of any license agreement is whether the use of the licensed information will generate new information that is of value. If so, provision should be made in the agreement for who will own this new information, when and how the new information will be shared between the parties, and how the information can be used. If the new information might be patentable, it is important to require the timely disclosure of the information between the parties so that no patent deadlines are missed.

4.54 One example of a business relationship that will often call upon the foregoing licensing principles is the franchisor/franchisee relationship. Typically, the franchisor will want to ensure that the franchisee is prohibited from disclosing its trade secrets. The franchisee may, in turn, require that its employees sign confidentiality agreements to protect the trade secrets.

4.55 Overall, a company wishing to license a trade secret should consider the nature of the trade secrets and/or know-how sought to be licensed, how the trade secret is recorded, the steps that have been taken to preserve the secrecy of the trade secret, and the form in which the trade secrets will be conveyed to the

27 See *Brulotte* v. *Thys Co.*, 379 US 29, 33 (1964).
28 See *Warner-Lambert Pharmaceutical Co.*, 178 F.Supp. 655, n. 25 above.
29 See 17 USC ss. 203(a) and 304(c) (2012).

licensee. It is also important to pay attention to employment agreements to ensure that they contain confidentiality obligations relating to the trade secret. Written company standards that protect trade secrets would also be helpful, particularly where ownership of the trade secret information may become an issue. It is advisable to clearly set out the ownership rights between or among the parties. The scope of use, especially with a software license, can be an important issue and should be clearly defined.

IV. PROTECTING AND MANAGING THE TRADE SECRETS OF ANOTHER

4.56 As noted previously, information flows in and out of businesses from a variety of sources. Some of the information is free for everyone to use, some constitutes the trade secret and confidential information of the business itself and some is information that is required to be kept confidential by various laws and legal doctrines or by social norms. Another type of information is the information of another that is received pursuant to a business relationship (such as from a licensor) that may or may not include a duty of confidentiality. Ideally, all categories of information used by a business will be identified for appropriate handling but, at a minimum, the information that must be kept confidential has to be identified so that appropriate security measures can be undertaken.

4.57 While most of the discussion in this book is from the perspective of the trade secret owner, it is also important for businesses to be mindful of trade secret protection when they are the recipient of another's trade secrets or confidential information. Whether as a licensee, vendor or otherwise, a company could be the recipient of another company's very sensitive information and thereby be exposed to potential liability for failing to adequately protect such information. Also, because there is tremendous responsibility associated with being entrusted with another entity's trade secrets, companies should think carefully about the information they are willing to receive under an obligation of confidentiality.

4.58 It is recommended that businesses take the position that they will not owe any duties to the owners of trade secrets or other business information that they receive unless it is agreed to in a written contract. Such a contract may take the form of a non-disclosure or licensing agreement or a simple letter agreement. However, because it is possible for implied duties of confidentiality to attach to certain relationships, discussed above, it is also important for the recipients of information to act in a manner that will not support a finding of an implied

agreement. Often, this requires training the employees who are apt to receive information in the proper response to oral and email requests for confidentiality.

4.59 As noted above, from an information owner's perspective, it is also important for a recipient of information to agree to specific security measures to protect such information so that it can be successfully argued that those measures were reasonable. From the recipient's point of view, however, it is important that it does not over-promise concerning the security measures it will institute. What security measures are needed should be tailored to the actual risks involved based upon the nature and intended use of the subject information. As a practical matter, the costs of such measures (including potential liability for breach of the duty of confidentiality) should not outstrip the value of the information to the recipient. If it does, the recipient should consider other means of properly acquiring such (or similar) information, as discussed below.

4.60 As further discussed in Chapter 5, once a company receives information that it agrees to keep confidential, it should institute processes to make sure that its employees and agents are aware of the nature and scope of any obligations of confidentiality and that they agree to abide by them. At a minimum, it is wise to have policies in place regarding the handling and storage of third party information in addition to the policies that are needed to protect the company's own trade secrets. For instance, the company might require that all such information received from third parties be conspicuously stamped or marked with appropriate legends and that those specially-marked documents be kept separate from (and perhaps require higher access levels than) all other documents.

4.61 A particular problem facing the recipients of trade secrets (like trade secret owners themselves) is the risk that trade secrets will be acquired by third parties that are not a party to the business relationship between the trade secret owner and the recipient. As discussed in Chapters 3 and 6, the knowledge requirement of US trade secret law poses problems when third parties come to possess trade secrets that were earlier misappropriated by someone else, for instance, as a result of a licensee's lax security standards. Generally, in order to establish misappropriation against a third party, it must be established that the third party either owed a duty of confidentiality to the trade secret owner or acquired the trade secrets by improper means.

4.62 Like a trade secret owner, the recipient of trade secret information should be focused on preventing the improper acquisition of trade secrets by both its

employees and third parties. If third parties are given access to such information, the initial recipient of the information should ensure that the third parties agree to a binding obligation of confidentiality. Generally, as discussed in Chapter 3, under US law a third party may be held liable for trade secret misappropriation if: (1) he knew or has reason to know of the wrongdoing by the direct misappropriator; or (2) he acquired the information under circumstances giving rise to a duty to maintain or limit its use. A third party may also be held liable in the case of accident or mistake where he knew or had reason to know that the information disclosed to him was a trade secret and that knowledge of it had been acquired by accident or mistake.

V. PROPER INFORMATION GATHERING

4.63 It is the public policy of the United States and most free-market economies that copying and imitation is not only allowed, but highly desirable.[30] This is because copying and imitation help to increase competition, reduce prices for consumers and often lead to improvements in goods and services. Thus, except where a product or device is protected by patent law, there is nothing legally or morally wrong with acquiring a product or device in the free market and then breaking it down to discover how it works.

4.64 As detailed in Chapter 3, the commentary to the UTSA and applicable case law in the United States has identified a number of 'proper' information gathering techniques that companies should understand as they consider whether and to what extent they wish to acquire information through a licensing arrangement or engage in their own research and development efforts. These include the recognized techniques of 'reverse engineering' and 'independent development' and the process of collecting publicly available information that is known in the business world as 'competitive intelligence'.

A. Reverse engineering

4.65 Reverse engineering is defined as 'starting with the known product and working backward to divine the process which aided in its development or manufacture'.[31] Unless restricted in an enforceable contract, as discussed above, the act of reverse engineering is not unlawful or otherwise wrongful as long as it is not tainted by trade secret information. As a US court explained: 'The relevant

30 See *Bonito Boats* v. *Thunder Craft Boats, Inc.*, 489 US 141, 146 (1989) (calling imitation and refinement though imitation the 'lifeblood of a competitive economy').

31 *Kewanee Oil Co.* v. *Bicron Corp.*, 416 US 470, 476 (1974).

inquiry is whether the means to obtain the alleged trade secret were proper or "honest", as opposed to being obtained by virtue of a confidential relationship with an employer'.[32]

4.66 Issues with reverse engineering tend to come up in two ways in trade secret cases. First, the ease with which something can be reversed engineered relates to the readily ascertainable prong of the definition of secrecy. If putative trade secret information can be easily ascertained from publicly available information, including products and services that are on the market, then the information is not 'secret' in the first instance. How easily information can be derived from publicly available information is the critical inquiry.[33] Second, the issue of reverse engineering arises when the defendant in a trade secret case argues that the information in his possession was acquired through reverse engineering, and therefore was not acquired through misappropriation.

4.67 As noted previously, an issue that has arisen in trade secret cases, particularly with respect to the licensing of computer software, is whether the ability to reverse engineer a publicly available product can be restricted by an express or implied contract.[34] Those who favour principles of freedom to contract argue that employers and other owners of trade secrets should be allowed to restrict their employees, vendors and customers from engaging in such acts.[35] On the other hand, such restrictions go against the public policy that favours the dissemination and use of public information and knowledge and, therefore, may not be enforceable.

B. Independent development

4.68 Independent development is the process by which individuals and companies develop their own inventions, creations and bodies of information. It is also known as research and development and differs from reverse engineering because it does not involve looking at a known (and publicly disclosed) product or service to try to ascertain the trade secrets and other proprietary information. Rather, as the label describes, it involves independent research efforts that rely upon one's general skill and knowledge and publicly available information.

---

32 See *Kadant, Inc.* v. *Seeley Mach., Inc.*, 244 F.Supp.2d 19, 38 (NDNY 2003).

33 See *CheckPoint Fluid System International, Ltd* v. *Guccione*, 888 F.Supp.2d 780, 797 (ED La. 2012).

34 See *Vault Corp.* v. *Quaid Software Ltd*, 655 F.Supp. 750 (ED La. 1987) (express license agreement restricting reverse engineering cited by plaintiff to bolster its trade secret misappropriation claims); *Chicago Lock Co.* v. *Fanberg*, 676 F.2d 400, 405 (9th Cir. 1982) (finding no implied duty to refrain from reverse engineering).

35 See Raymond Nimmer, *Information Law* (2002), paras 2.12[1], 5.05[3] and 5.11[4][b].

4.69 As with the process of reverse engineering, the process of independent development can be inappropriately tainted by the knowledge of others, such as employees of a company who were exposed to the trade secret and confidential information of a former employer. To avoid such taint, it is generally recommended that companies that engage in independent development institute processes and procedures to prevent any trade secret and confidential information from being disclosed or used by researchers. This is often accomplished by establishing a 'clean room' where only new or publicly disclosed information is allowed and where employees with knowledge of the trade secrets of others are excluded.

C. Competitive intelligence

4.70 Unbeknownst to many lawyers, there is a robust and organized group of companies and professionals that are in the business of 'competitive intelligence'. Often, in order to compete effectively, companies need to acquire information about their competitors with respect to, for instance, prices charged and type of products sold. Thus, most major corporations engage in competitive intelligence on a regular basis and to do so they frequently seek the services of firms and individuals that specialize in competitive intelligence activities. As noted earlier, competition is a good thing because it helps to lower prices and can improve the quality of goods and services.[36] Thus, competitive intelligence is also a good thing unless it goes too far and becomes improper.

4.71 Competitive intelligence about another company can be acquired from a number of legitimate sources which, as explained in Chapter 3, the comments to the UTSA explicitly recognize as 'proper means'. This includes obtaining information from required government filings, industry and company websites and blogs, trade journals and newspaper reports, patent filings, trade shows and Freedom of Information Act (FOIA) requests. As long as these efforts focus on publicly available or readily ascertainable information, they are not improper even if the end result is the loss of business profits due to increased competition. Sometimes, however, actions that are believed to be lawful acts of competitive intelligence constitute actionable trade secret misappropriation.[37]

4.72 Companies that engage in competitive intelligence should be mindful that their activities do not cross the line and become improper acts of corporate espionage. As discussed in more detail in Chapter 6, espionage is actionable as a criminal and civil matter. Indeed, it is directly covered by US federal law under

36 See *FTC* v. *Superior Court Trial Lawyers Association*, 493 US 411, 423 (1990).

37 See e.g., *MicroStrategy, Inc.* v. *Business Objects, SA*, 331 F.Supp.2d 396 (ED Va. 2004).

the Economic Espionage Act, which provides substantial penalties, including imprisonment, for foreign and domestic espionage.

VI. IDEA SUBMISSION CASES

4.73 As noted earlier, when a company is sharing information with another, it is in its best interest to be able to establish the existence of an express or implied duty of confidentiality. When it is on the receiving end of information, however, it is better from an information management and potential liability standpoint that there are no restrictions with respect to the handling of such information. One particular situation where this problem arises is in what is known in the United States as 'idea submission' cases (a type of breach of confidence case in the United Kingdom).

4.74 In a typical idea submission case, an individual who developed an idea or invention that he thinks would be of value to a company, submits that idea or invention to the company (usually unsolicited) and later alleges that the company used the idea without compensation. These cases can involve ideas of potential interest to the entertainment industry, such as a concept for a movie or a new television show, but they can also involve any idea that may be of interest to business, such as ideas for new products.

4.75 Unfortunately for businesses, idea submission cases often involve power differentials between the plaintiff 'idea man' and the alleged misappropriator that can prove difficult for a defendant in an idea submission case to overcome due to the common perception that the idea man is being taken advantage of by a greedy corporation.[38] Thus, in the absence of a suitable idea submission policy that alerts the idea man not to expect compensation or confidentiality, litigation can result once the idea man believes that his idea is being used.

4.76 In the United States, idea submission claims will often be brought as breach of contract or common law misappropriation claims. However, to the extent an idea was kept as a trade secret before it was disclosed to a prospective user or purchaser, there is a possible overlap between idea submission claims and trade secret claims. If the idea qualifies for trade secret protection, then the idea generator is likely to assert a trade secret misappropriation claim, usually of the breach of confidentiality variety. In such cases, it is not enough for the plaintiff to prove the existence of a duty of confidentiality; the plaintiff must also prove that the subject information was a trade secret.

38 See *Rogers* v. *Desa International, Inc.*, 183 F.Supp.2d 955, 957–8 (ED Mich. 2002).

4.77 Of course, an idea man who relies upon a trade secret theory has the burden of proving all of the essential elements of a claim for trade secret misappropriation. Unlike the employment relationship, which is an ongoing business relationship, proving reasonable efforts to protect an idea can be a challenge for the plaintiff idea generator. Without a pre-disclosure agreement, the plaintiff in an idea submission case will have difficulty proving that the idea, which it voluntarily communicated to the defendant, qualifies as a trade secret. In cases where there was a pre-disclosure agreement, the main question under the reasonable efforts analysis becomes whether the agreement, alone, is sufficient.

4.78 In the United States, idea submission cases are not necessarily dependent on the existence of a trade secret or even a novel idea. If the plaintiff in an idea submission case can prove the existence of an express or implied contract, some courts are willing to provide recovery for ideas that would not qualify for trade secret protection.[39] However, unlike the employment relationship or an on-going business relationship, the short-term nature of the relationship is often a factor that weighs against finding an implied duty of confidentiality in idea submission cases.[40] As in all trade secret cases, a distinction should be made in idea submission cases between an implied contractual obligation that may serve as the basis of a breach of contract claim and an implied duty of confidentiality that is needed to support a trade secret misappropriation claim.[41] Contractual claims like these are not precluded by the enactment of the UTSA, but a trade secret claim may be precluded by the idea man's failure to prove the existence of a trade secret due to his voluntary disclosure of the idea.

4.79 Although it is often said that novelty is not a requirement for trade secret protection, in the United States it is more appropriate to recognize that novelty in the patent sense is not required. Generally, courts will not support attempts to protect common, trivial or well-known facts as protectable ideas or trade secrets. Thus, courts will examine both the concreteness and novelty of an idea in an attempt to distinguish between information that can be the subject of a successful idea submission claim and that which cannot. As discussed in Chapter 3, pursuant to the UTSA, ideas that are generally known and readily ascertainable cannot be trade secrets. Similarly, ideas that are generally known cannot serve as the basis for an idea submission claim because the public availability of the ideas suggests that they would have no value to the buyer and, therefore, do not provide sufficient consideration for the alleged contract.

---

39 See *Reeves*, 926 P.2d, n. 7 above, at 1136.

40 See *Smith*, 833 F.2d, n. 14 above, at 580–1.

41 See generally, 926 P.2d 1130, n. 7 above (explaining the requirements for claims based upon implied contracts).

VII. IMPLEMENTING AND MONITORING A TRADE SECRET PROTECTION PLAN

4.80 While potential causes of action for breach of confidentiality and trade secret misappropriation are tools for protecting trade secrets and other confidential information in business relationships (as described above), there is nothing better that a well-planned and properly executed trade secret protection plan that is applied with vigilance.

4.81 The first part of any trade secret protection plan is to identify the specific information that qualifies as trade secrets and any other information that is sought to be protected. For both practical, legal and management purposes, it is important that companies do not take the position that every bit of information that they utilize in their business is a trade secret. Such a claim can be grossly exaggerated and, more importantly, it fails to put employees on notice of the actual information that can qualify for trade secret protection. Courts in the United States have shown reluctance to sanction the overbroad assertion of trade secret rights when to do so would limit the mobility of employees. More importantly, the more information that is identified for protection, the more difficult and costly it will be to manage the trade secret protection programme and the more difficult it will be to identify and protect real trade secrets.

4.82 In addition to the written agreements, discussed above, some typical safeguards that should be part of every protection plan include: (a) ensuring that access to areas that contain trade secret information are appropriately limited and controlled; (b) locking and guarding trade secrets and using detection devices to determine when there may have been intrusions; (c) restricting and segmenting trade secrets so that access is provided to only the parts of the trade secret necessary for the individual employee or subcontractor to perform the task assigned; (d) labelling materials as confidential or trade secrets and posting visible warnings; (e) using secure technological protections such as encryption and passwords for electronically stored trade secret information; (f) auditing trade secrets and access to them on a regular basis; (g) teaching and reminding employees about the importance of protecting trade secret information; (h) instituting policies that govern employees, not only in the workplace, but at home, and in areas outside of the office where employees may also work and have access to proprietary information; and (i) ensuring that third parties, subcontractors, consultants and vendors that have access to trade secret information sign confidentiality agreements and observe appropriate safeguards when using trade secrets.

4.83 When both developing and implementing a trade secret protection plan, it is important to consider human behaviour in conjunction with whatever legal and technological tools may be utilized and to think holistically about the necessary approaches to trade secret protection. In addition to careless or accidental disclosures, businesses must also protect against individuals who maliciously or intentionally set out to acquire trade secrets through illegal means. These can include hackers who outsmart the technological barriers that are in place and individuals who engage in corporate and foreign espionage. Thus, consideration of the interaction and influence of human behaviour should be part of any comprehensive trade secret protection scheme. The key to trade secret security is proactivity rather than reactivity.

4.84 Consistent with the need to consider human behaviour in a trade secret protection plan, account should be taken of the culture, customs and social norms of various societies. This is especially noteworthy for companies doing business in other countries. In order for intellectual property rights, including trade secret rights, to be meaningful, it is critical to understand the differences in value systems, organizational structures and heritage of various countries and act accordingly.

4.85 In some countries where misunderstanding of and disregard for intellectual property rights might be the rule rather than the exception, it is important to consider the cultural barriers and differences that might make it difficult to implement a trade secret security programme. For instance, in China, because express laws to protect intellectual property rights have only been in effect for several decades, the average business person or employee may be unaware of the nature and scope of those laws and may need to be educated. To the extent that there is a disconnect between US (and other developed countries) use of intellectual property rights and the values attendant in those laws versus the values of developing countries, practical strategies for obtaining compliance may ultimately be more useful and successful, instead of reliance on enforcement. In other words, trade secret protection should not be viewed as merely an enforcement problem that arises once a breach of confidentiality occurs, but a matter of day-to-day compliance as well.

5

TRADE SECRECY IN EMPLOYMENT RELATIONSHIPS

I. INTRODUCTION

5.01 Business-to-business relationships are not the only, or even the principal, type of relationship that trade secret owners must consider when developing a trade secret protection strategy. Statistically, most of the trade secret cases filed in the United States arise out of the employment relationship. The typical story involves an employee who leaves the employ of one company to work with a competitor or to start her own business and is accused of taking her former employer's trade secrets with her. Without proper planning, this scenario can result in bad outcomes for a trade secret owner, not only from a legal perspective but from a practical perspective.

5.02 As with business-to-business relationships, the existence of a duty of confidentiality is a key component of any trade secret protection strategy related to employees. However, just because an individual works for a company does not mean that they owe a duty of confidentiality with respect to specific (or any) trade secrets. This is because a critical component of trade secret protection in the workplace requires employees to be informed of the applicable expectations of secrecy with respect to the information that they handle. Sometimes an implied duty of confidentiality will be found, but not always. Thus, as with business-to-business relationships, the best practice is to obtain an express written confidentiality agreement from each employee who is given access to

trade secrets and other proprietary information. At a minimum, efforts should be undertaken to inform employees of the employer's expectation of confidentiality and to identify the information that is the subject of such expectation.

5.03 While obtaining an express written agreement of confidentiality from key employees is important, no company should rely upon an agreement to provide complete protection for its trade secret information. Steps must also be taken to ensure that employees who are entrusted with trade secret information can be trusted to keep it secret. Typically, this is accomplished through the use of background checks and other security clearance procedures and by educating employees about their responsibilities related to trade secret and other business information. The monitoring of employee activities, particularly with respect to higher level employees who have day-to-day access to trade secrets, is also needed.

5.04 This chapter begins by exploring how duties of confidentiality can be formed in employment relationships. In contrast to business-to-business relationships, it is generally easier to establish implied duties of confidentiality in the employment relationship because of the employee's duty of loyalty, but the best approach for employers who wish to strengthen and clarify their position relative to employees is to enter into signed contracts that make the rights and responsibilities of the parties clear. Generally, these contracts will take the form of confidentiality agreements, non-solicitation agreements, non-compete agreements and employment agreements, as discussed below. However, because these contracts often involve restraints on trade, courts will scrutinize them carefully to determine whether they are reasonable and to ensure that they do not unfairly burden the employee.

5.05 Other issues that are discussed in this chapter include the public policy limits that are placed upon agreements with employees, the inevitable disclosure doctrine of US trade secret law and the ownership of employee created inventions. In considering how to structure relationships with employees, companies must be aware that public policy issues loom large, particularly in trade secret cases. One important policy that courts must often balance is society's interest in the mobility of labour. Another concerns the general skill and knowledge that individuals learn throughout the course of their lives, education and work experience and the practical need for employees to use their skills and knowledge in successive jobs. Additional policy interests, such as promoting fair competition between businesses and protecting employers against breaches of confidence by former employees, also enter into the balance. Finally, in the United States, as elsewhere, the law and practices governing

employment, including the potential influence of employee unions, must be taken into account.

5.06 The chapter ends with a discussion of practical tips for the selection, training and oversight of employees. Its key message is that obtaining an express non-disclosure agreement from employees is not enough; care in selecting and supervising employees is also needed.

II. ESTABLISHING A DUTY OF CONFIDENTIALITY WITH EMPLOYEES

5.07 As detailed in Chapters 2 and 3, one type of trade secret misappropriation under both the Uniform Trade Secrets Act (UTSA) and Article 39.2 of the TRIPS Agreement involves the wrongful use or disclosure of trade secret information in violation of a duty of confidentiality. In fact, most trade secret claims involve this type of wrongdoing, principally because it is the means by which employees are typically held liable for trade secret misappropriation. The critical questions in such cases are: (1) whether the employee owes a duty of confidentiality to her employer; and, if so (2) the scope and nature of that duty.

5.08 In practice, how duties of confidentiality are defined and imposed in a given case will often depend on the facts of the case and whether the employee is in the type of position where a need for confidentiality is evident. Some jurisdictions, like California, tend to favour the rights of employees relative to employers, and thus, are more likely to use public policy arguments to limit restrictions on employee mobility.[1] Other jurisdictions, while mindful of the benefits of employee mobility and the potential detriments of restrictive covenants, are more receptive to employer claims, particularly if the subject employee entered into a written confidentiality or non-compete agreement with his employer.[2]

A. Implied duties of confidentiality

5.09 As introduced in Chapters 3 and 4, in the absence of a written confidentiality agreement, courts are left to interpret the facts surrounding a given relationship to determine whether an implied duty of confidentiality exists. But the employment relationship is a special relationship which, while more likely to impose obligations of confidentiality on employees, will also be more closely scrutinized for fairness.

---

1 See e.g., *Metro Traffic Control, Inc.* v. *Shadow Traffic Network*, 22 Cal. App. 4th 853, 859–60 (Cal. Ct App. 1994).
2 See e.g., *National Reprographics, Inc. v. Strom*, 621 F.Supp.2d 204, 229 (DNJ 2009).

5.10 In many countries, including the United States, the employment relationship imposes a number of statutory, common law and implied obligations upon both the employer and the employee,[3] which often come to bear directly on the law of trade secrecy. One of these obligations is the implied duty of loyalty (discussed below) that employees owe to their employers and that is largely a matter of employment law in the United States. From this concept often springs an implied duty of confidentiality that employees owe to employers with respect to employer-owned trade secrets and other business information.

5.11 The general rule in the United States is that an employee stands in a confidential relationship with his or her employer with respect to the employer's confidences. Thus, an employee's duty not to disclose the secrets of her employer may, even without an express contract, be implied from the employer/employee relationship. However, depending upon the nature of the employment, the actual scope of the duty of confidentiality can vary greatly among employees. There is also the practical question for trade secret purposes whether (and if so to what extent) the applicable duty of confidentiality extends beyond an employee's employment with a particular company.

5.12 Some courts in the United States have held that an employee's implied duty of confidentiality applies to an employer's trade secrets even after the employee no longer works for the employer. Other courts have gone so far as to treat the employee's duty of confidentiality to the employer as a fiduciary obligation. Thus, while arguments might be made to establish an implied duty, the practical problem is that without an express and enforceable obligation of confidentiality, an employer cannot be certain how far and for how long a duty of confidentiality will extend.

5.13 While plaintiffs in trade secret cases are inclined to argue for a broad application of equitable principles to establish a duty of confidentiality, the focus of the analysis in most US cases is on the precise relationship between the trade secret owner and the alleged misappropriator. In the employment context, the focus is on the nature and status of the employee's work and whether the employee is given access to confidential information. This is particularly true with respect to low-level employees and employees who have no knowledge of either the existence of trade secrets or the expectation of confidentiality. Thus, while some authorities in the United States argue that the mere sharing of information with another who knows the information is considered to be a trade secret can create a duty of confidentiality, with respect to employees, courts often insist on a higher degree of proof of the existence of an implied

3 See e.g., Mark A. Rothstein *et al.*, *Employment Law* (4th edn 2010), pp. 3–4.

duty of confidentiality. If employees of a company did not know that they were given access to trade secrets and that confidentiality was expected, arguably no duty of confidentiality should attach.

5.14 In the United States, the *Restatement (Third) of Unfair Competition* provides that an implied duty of confidentiality arises in trade secret cases when the circumstances justify the conclusion that the person receiving the information knew or had reason to know that the disclosure was intended to be in confidence and the trade secret owner was reasonable in inferring that the recipient of the information consented to an obligation of confidentiality.[4] This requires examination of: (1) the circumstances surrounding any disclosure; (2) the recipient's state of mind; and (3) the reasonableness of the trade secret owner's actions. It also requires application of principles of contract law that distinguish between express agreements, implied-in-fact agreements, and implied-at-law agreements.

5.15 Generally, to establish an implied-at-law duty of confidentiality in a trade secret case an employer should present evidence of the nature and character of the relationship between the parties and the circumstances that led to the disclosure of the putative trade secrets; the goal being to show that the equities demand a finding of an implicit promise of confidentiality. Evidence disclosed in written and oral communications may be highly relevant to determining whether a duty of confidentiality should be implied. Additionally, all of the efforts that a trade secret owner should engage in to meet the reasonable efforts requirement of trade secrecy may support a finding of an implied duty of confidence, provided that the subject employee was aware of such efforts. This would include, for instance, limiting access to important information and marking such information as 'confidential'.

5.16 Where an express contractual agreement of confidentiality existed between the parties, it usually cannot be controverted by an implied agreement, and its terms will serve to define the duty of confidentiality, if any.[5] In other words, an implied duty of confidentiality will generally not be found where there is an express agreement on the same subject. Thus, while it is generally recommended that trade secret owners enter into express confidentiality agreements with their employees, care must be exercised to ensure that the terms of that agreement are sufficient to protect the employer's interests.

4 *Restatement (Third) of Unfair Competition*, s. 41(b).

5 See *Nilssen* v. *Motorola, Inc.*, 963 F.Supp. 664, 679–82 (ND Ill. 1997).

5.17 While the precise scope and nature of any duty of confidentiality should differ depending upon the particular facts of a case and the law of a given jurisdiction, it often includes a duty to maintain the confidentiality of known trade secrets.[6] In some jurisdictions, it may also require employees to maintain the confidentiality of proprietary business information that does not meet the definition of a trade secret.[7]

B. Contractual duties of confidentiality

5.18 Because establishing a duty of confidentiality with an employee (or any other person who may come to possess trade secrets) is of critical importance under trade secret law, and the scope and nature of any implied obligation may be limited, it is generally recommended that trade secret owners use contractual confidentiality agreements wherever possible. These contracts aim to protect company trade secrets and confidential business information. However, courts will scrutinize the reasonableness of these agreements in deciding whether to enforce them, particularly when they limit the rights of employees to pursue new job opportunities and career advancement.

5.19 If a trade secret owner wants to impose a duty to maintain the confidentiality of information on its employees, the best way to do so is to get the promise in writing before any disclosure occurs.[8] This can take the form of a confidentiality clause in an agreement that deals primarily with other matters (for instance, a clause in an employment agreement) or a separate 'confidentiality agreement' or 'non-disclosure agreement' (NDA).

5.20 Confidentiality or non-disclosure agreements in the United States generally express in writing the common law obligation of an employee to maintain his employer's confidences, but they are also helpful for: (1) delineating the confidentiality expectations between the employer and employee, particularly with respect to trade secrets; (2) showing that the employer takes trade secret protection seriously; and (3) demonstrating the employer's reasonable efforts to maintain the secrecy of its confidential information. As with contracts generally, they can also be used to subject the employee to personal jurisdiction in a particular state or country and to define the applicable law and available remedies for breach of the agreement, including injunctive relief.

---

6 See *Town and Country House and Homes Service, Inc.* v. *Evans*, 189 A.2d 390 (Conn. 1963).

7 See e.g., *Willis of NY, Inc.* v. *DeFelice,* 750 NYS 2d 39, 42–3 (NY App. Div. 2002).

8 See *B.F. Goodrich Co.* v. *Wohlgemuth*, 192 NE 2d 99, 105 (Ohio Ct App. 1963) ('Th[e] written contract expressly binds the employee … not to misuse special confidential knowledge of trade secrets secured by him while the contractual relationship of employment existed').

5.21 In a typical NDA, an employee acknowledges that the confidential information (as defined in the agreement) is the sole property of the employer and agrees not to use or disclose such information except in the course of employment for the benefit of the employer. Confidential information is often broadly defined in NDAs and other forms of confidentiality agreements to include all kinds of business information, not limited to trade secrets. For instance, a typical definition might include 'all business, proprietary, confidential and trade secret information and know-how'. While, on one hand, such a clause appears to benefit an employer due its breadth, on the other hand, it can fail in actually informing employees of the identity of trade secrets.

5.22 In the United States and elsewhere, merely listing information or categories of information in a confidentiality agreement cannot transform the information into a trade secret. Trade secrets, if they exist at all, have an independent legal existence. The other requirements for trade secrecy (see Chapter 3) must be met and should be kept in mind when devising a trade secret protection strategy. For the other information that is defined in a confidentiality agreement (that which does not independently qualify for trade secret protection), the only remedy for breach of the confidentiality agreement is likely to be a breach of contract claim.

5.23 Confidentiality agreements also typically require the employee to promise that during and after her employment she will not disclose the information to anyone outside the company or use it for her own benefit or for the benefit of others without the company's prior written permission. In well-written NDAs, the employee will further promise to return to the company all documents or other materials relating to her work upon termination of the employment relationship and that the employer has the right to search the employee's desk, computer and personal belongings for employer-owned information.

5.24 Because NDAs may bind a person to confidentiality even after trade secret protection has expired (for example, due to public disclosure), an employee signing such an agreement might want to ensure that exclusions apply which would not limit disclosure post-expiration of the secret (discussed as 'carve-out clauses' in Chapter 4).[9] Or the employee may wish to limit the post-employment confidentiality obligation to a specific number of years. From the trade secret owner's perspective, however, since trade secret protection is perpetual as long as the information is kept secret, the owner of the information might be reluctant to agree to a fixed term of confidentiality in a contract.

9 See Jane Clark and Lisa R. Lifshitz, *Technology Transfer and Licensing* (2008), para. 13.2(1).

5.25 For companies that utilize the Internet and allow employees to use their own devices (including laptops, tablets and cellphones), it is also advisable for NDAs to extend to such devices and detail if, how and when company trade secrets can be transmitted by and stored in such devices. In other words, it is usually not enough to exact a simple promise of confidentiality from employees without addressing where and how company information is actually used and shared. The better practice is to anticipate how and where employees are likely to use and share company information and to include specific instructions and guidelines for how such information is to be handled and secured. Failure to do so may make it difficult to prove that an employee breached his duty of confidentiality or, worse, may result in a finding that a company's trade secret protection measures were not reasonable and, therefore, that no trade secrets exist in the first instance.

5.26 When developing rules and procedures concerning the use and sharing of trade secrets by employees, it is important to consider how information must flow within an organization and the potential benefits of collaboration both among employees within a company and with third parties. It is easy for attorneys who advise clients on trade secret matters to recommend a variety of efforts that are designed to protect such secrets, but if the end result is the lock-down of information in ways that make the operation of a business less successful or less efficient, such efforts are counter-productive. Some companies and some industries prefer an open innovation model of conducting business, while others wish to carefully guard their secret formulas and processes. Confidentiality agreements must be drafted with an understanding of the particular goals and business practices of the client.

C. Employment agreements

5.27 Frequently, particularly where trade secret protection is an afterthought, companies will attempt to rely upon a confidentiality clause in an employment agreement or an employee policy manual to establish a contractual duty of confidentiality. While it is always advisable to include confidentiality provisions in employment agreements and policies because of their educational value, they do not always suffice to establish a binding duty of confidentiality and should not be relied upon for such purposes. This is because general employee policies do not typically identify the specific employees or classes of employees that are subject to duties of confidentiality and in this sense are over-broad. Additionally, general employee policies are usually not helpful in identifying the information that is claimed as trade secrets and thereby fail to put employees on notice of the precise information sought to be protected. As explained in

Chapter 3, the failure of a company to identify its trade secrets and engage in tailored efforts to protect those secrets can be fatal to a claim of trade secrecy.

III. EMPLOYEE DUTY OF LOYALTY

5.28 Often in trade secret cases involving employees in the United States and elsewhere, employers will invoke other principles of law in an attempt to bolster the argument that there is an implied duty of confidentiality. In particular, they may rely upon the 'duty of loyalty' that is said to exist between an employer and an employee.[10] Or, depending upon the nature of the employment, they may argue that the employee owed a fiduciary duty to his employer.

5.29 Generally in the United States, while working for an employer, employees owe a duty of loyalty to their employer and thus must not behave in a manner that would harm the employer.[11] However, this duty traditionally and usually relates to conflicts of interest, such as working on personal matters at work or engaging in efforts to open a competing business and, as a practical matter, may not adequately advise individual employees of the need to protect specific information claimed to be a trade secret. Thus, care should be taken to ensure that the existence of the duty of loyalty (or 'other' duties) does not subsume the trade secret analysis and that such a duty is not relied upon as a substitute for a trade secret protection programme. Defendants in trade secret cases will often argue that the trade secret analysis requires a finding that the defendant was under the specific duty to protect particular trade secrets.

5.30 Additionally, an issue that often arises concerning duties of confidentiality and duties of loyalty concerns the precise definition and scope of those duties. Employers frequently assert that duties of confidentiality and loyalty should be interpreted broadly to restrict employees from using or disclosing a wide variety of proprietary information. This sometimes includes solicitation of customers and the use of other competitive information to which the employee had access. Ultimately, how the implied duties of confidentiality and loyalty are defined will depend on the facts and circumstances of the particular case, as well as the applicable law of each jurisdiction. To minimize definitional uncertainty and to avoid costly litigation, appropriate written agreements should be utilized instead.

---

10 See *Scanwell Freight Express STL, Inc.* v. *Chan,* 162 SW.3d 477, 481 (Mo. 2005).

11 See Brian M. Malsberger, *Employee Duty of Loyalty: A State-by-State Survey* (4th edn 2009 and Supp. 2010).

IV. OTHER AGREEMENTS TO PROTECT TRADE SECRETS

5.31 In the United States, employees are free to work for whomever they wish and to pursue a livelihood and most employment relationships in the United States are 'at will'. However, in some circumstances, trade secret and other principles of law allow employers to restrict the fundamental right of employees to move from employer to employer or otherwise pursue their calling. Because these efforts constitute restraints of trade, courts will pay close attention to efforts by employers to use trade secret rights as a means to prevent an employee from working for a competitor or exercising their entrepreneurial spirit to open a competing business.

5.32 From an employer's perspective, restrictive covenants, including confidentiality agreements, can enhance a company's legitimate interest in its trade secrets and other assets, such as goodwill. Companies often need such covenants to encourage investment, protect innovation and promote competition. Additionally, these agreements typically contain provisions recognizing that any breach of the employment agreement would cause irreparable harm for which the company would have no adequate remedy at law, and that in the event of any such breach, the company would have the right to seek an injunction. They can also include arbitration and choice of law clauses.

5.33 The enforceability of restrictive covenants, even if designed to protect trade secrets, depends upon the laws of each jurisdiction and the particular language of the restrictions. Generally, agreements that are designed to govern the employment relationship and the use of information during employment are given greater leeway. Post-employment covenants requiring that an employee maintain secrecy, refrain from soliciting customers or employees and not engage in certain competitive activities are subject to greater scrutiny. So-called 'grant-back' clauses that require former employees to assign inventions that they developed after their term of employment are particularly likely to be scrutinized.

A. Non-compete agreements

5.34 Non-compete (or non-competition) agreements are utilized by employers when they wish to restrict employees from working for competitors. By entering into a non-compete agreement, the employee usually agrees that for a specified period of time after the end of his employment he will not work for any company which is a competitor of the employer; or, the language of the non-competition agreement may be worded such that an employee agrees not to work in a particular field. The general rule is that these agreements must be

designed to protect legitimate business interests of the employer because of the very restrictive nature of these agreements on the employee's freedom to work. What constitutes a legitimate interest is a subject of debate among courts, policymakers and commentators.

5.35 Whether the protection of trade secrets is a legitimate business interest is the key issue in trade secret cases. In the United States, trade secrets play a key role in non-compete agreements because the tying together of an obligation to maintain secrecy with a promise not to compete can make non-compete agreements enforceable in most, but not all states. A related issue is whether the protection of business information not meeting the definition of a trade secret (as discussed above with respect to confidentiality agreements) is a legitimate interest that can justify a non-compete agreement.

5.36 Because of the direct restrictions that are imposed on employee mobility, non-compete agreements (or clauses) are generally more controversial than confidentiality agreements. There is an obvious tension between competing policies: the employer's freedom to contract to avoid the challenge and uncertainty of litigation versus society's interest in an individual's freedom to seek new employment. Because of this tension, the policies of individual US states and countries vary as to the enforceability of non-compete agreements. They are typically enforced when entered into in conjunction with the sale of a business, but may not be enforced when designed only to protect trade secrets, goodwill or general business information.

5.37 In addition to the above caveats, some general rules apply to non-compete agreements both inside and outside of the United States. First, even if they are designed to protect some legitimate interest, non-compete agreements will be enforced only if deemed 'reasonable'. In determining reasonableness, courts often consider: (1) the duration of the restrictions (generally one–two years is the maximum courts will enforce); (2) the geographic scope of the restrictions (courts often examine the area in which the employee operated, which is likely to be the area in which the employee would have some opportunity to affect the employer's goodwill); (3) the nature of the interest to be protected; and (4) in trade secret cases, how quickly trade secret rights may diminish.

5.38 Second, in some jurisdictions, even if a non-compete agreement appears overly broad, courts will modify the restrictions so as to make them reasonable as long as the transaction is not otherwise tainted with unfairness.[12] This process is

12 See e.g., *Proudfoot Consulting Co.* v. *Gordon,* 576 F.3d 1223, 1231 (11th Cir. 2009); *Simpson* v. *C & R Supply, Inc.*, 598 NW.2d 914, 920 (SD 1999).

often referred to as 'blue-pencilling'. Jurisdictions that follow this process will strike out and replace provisions of the agreement deemed to be unreasonable, but they will not add terms and conditions that were not originally part of the parties' agreement.[13] Jurisdictions that do not follow this process may declare the entire agreement void and unenforceable, thereby placing a premium on the fairness of all provisions of an agreement.

5.39 Third, as with contractual agreements generally, non-compete agreements usually require consideration for the employee's promise not to work for a competitor. If signed at the beginning of the relationship, most courts in the United States find that the employment itself provides the consideration, but this may not be true in all countries. If a non-compete agreement is signed after the employee begins work, consideration might exist and be deemed sufficient in the United States if it was understood from the beginning that such an agreement would be a condition of the job. However, some courts in the United States have held that mere continuation of at-will employment is not enough consideration for a non-compete agreement signed during the term of employment.[14] Thus, the employer would need to provide fresh consideration to the employee in the form of a lump sum payment or a salary increase. Thought must also be given to the impact of employment contracts and union agreements on the need for and timing of additional consideration. Also, in some countries, it may be necessary to provide compensation that is equivalent to the salary the employee would have received during the period of non-competition.

5.40 Fourth, when the employer who signed an existing non-compete agreement changes through merger or acquisition, the agreement might not continue without the employee's consent, unless there was an assignment clause in the agreement.[15] Some courts in the United States have held that an assignment clause itself requires separate consideration, especially if the new employer inherited the non-competition agreement from an asset purchase agreement rather than through a merger.[16]

5.41 Fifth, non-compete agreements are an exception to the general preference of companies for at-will employment and in this regard are likely to impose additional obligations on the employer as well as the employee. In particular, they may be interpreted as establishing a term contract of employment that is more difficult to terminate than an at-will contract. Thus, they should not be used for all employees, but only for those employees who may engage in

13 See Richard A. Lord, *Williston on Contracts* (4th edn 1990), para. 13:25.

14 See *Guercio* v. *Product Automation Corp*., 664 NW.2d 379, 386–7 (Minn. Ct App. 2003).

15 See *OfficeMax, Inc.* v. *County Qwick Print, Inc.*, 709 F.Supp.2d 100, 110 (D Me. 2010).

16 See *Traffic Control Services, Inc.* v. *United Rentals Northwest, Inc.*, 87 P.3d 1054, 1057 (Nev. 2004).

competitive activities that are likely to be harmful (at least in the short term) to the employer.

5.42 Many US states recognize and enforce non-compete agreements as long as the restrictions are reasonable in view of the totality of the circumstances.[17] But courts will often take into consideration the financial hardship to the employee if the non-compete agreement is enforced. A few states only recognize these covenants under narrow and specified circumstances, with a presumption against enforceability.[18] California, for example, is notable for its strong and long-standing public policy that declares non-compete agreements void and unenforceable except in very limited situations not including the protection of trade secrets.[19]

B. Non-solicitation agreements

5.43 Another type of restrictive covenant that implicates trade secret protection is a non-solicitation agreement (or clause). These are generally less controversial than non-compete agreements because they do not preclude an employee from working for a competitor. Rather, they limit the customers that can be solicited by a former employee[20] and may also prevent the former employee from 'raiding' the employees of the former employer.

5.44 In the United States, an employee who leaves a company to join a competing enterprise can be contractually restricted from soliciting business from the former employer's customers, provided that the restrictions are reasonable. Additionally, in the right circumstances, an implied duty of non-solicitation may be found. Courts in the United States often draw a distinction between solicitation of customers, which directly affects the former employer's legitimate interest in its goodwill, and solicitation of employees (offering less protection). The nature of the employment and the interests of the customer also play a role in the analysis, with customer service professions like lawyers and physicians having more leeway to contact former customers due to the personal nature of those relationships. In some cases, the fact finder must determine whether a former employee was merely announcing a job change to the former employer's customers (not actionable) or actively soliciting them for their business (actionable).[21]

---

17 See *Campbell Soup Co.* v. *Desatnick*, 58 F.Supp.2d 477, 489 (DNJ 1999).

18 See *Paramount Termite Control Co., Inc.* v. *Rector*, 380 SE.2d 922, 924 (Va. 1989).

19 See California Business and Professions Code, s. 16600; *Edwards* v. *Arthur Andersen, LLP*, 189 P.3d 285 (Cal. 2008).

20 See *Digitel Corp.* v. *Deltacom, Inc.*, 953 F.Supp. 1486, 1495 (MD Ala. 1996).

21 See e.g., *USI Insurance Services, LLC* v. *Miner*, 801 F.Supp.2d 175, 191–2 (SDNY 2011).

V. INEVITABLE DISCLOSURE DOCTRINE

5.45 The doctrine of inevitable disclosure is a controversial doctrine within the United States and is typically raised where an employee of one company goes to work for a competitor, often under circumstances where there is no written non-compete agreement. Usually, the employee will readily admit that he is under an ongoing duty of confidentiality to his former employer, but the former employer is concerned that the employee's new job responsibilities make the disclosure of its trade secrets 'inevitable'. To prevent such disclosure, the former employer typically is not satisfied with an injunction precluding the disclosure of its secrets and instead wants an injunction to prevent its former employee from working for the competitor.[22] In effect, the former employer is asking the court to imply a non-compete agreement.

5.46 Because of the social importance of employee mobility and concerns about non-compete obligations, courts in the United States tend to approach inevitable disclosure cases with great care. Whether or not a particular court will accept the inevitable disclosure doctrine is often tied to the state's policies regarding non-compete agreements. Many states have applied the doctrine, other states recognize it in only very limited circumstances and some (like California) have rejected it outright.[23] Where applied, the inevitable disclosure doctrine provides a powerful weapon under trade secret law because it permits an employer to do that which it would not otherwise be entitled to do under the auspices of employment law: restrict an employee without a non-compete agreement and without additional compensation.

5.47 Although the inevitable disclosure doctrine can be used in cases where a non-compete agreement was executed, its use in those cases is not as controversial as in cases where the employer did not obtain an explicit non-compete agreement from the employee. In those cases, the doctrine creates a policy tension between the employee's right to move freely and pursue his or her livelihood and the employer's right to protect its trade secrets. Indeed, it appears to go against the at will doctrine, an important tenet of US employment law. The employment at will doctrine provides that without an agreement to the contrary, an employee may leave his or her employer at any time and for any reason.[24] Similarly, an employer may terminate an employee at any time, for any reason.

---

22 See *PepsiCo, Inc.* v. *Redmond*, 54 F.3d 1262 (7th Cir. 1995).

23 See *Whyte* v. *Schlage Lock Co.*, 101 Cal. App. 4th 1443, 1462–3 (Cal. Ct App. 2002) ('The chief ill in the covenant not to compete imposed by the inevitable disclosure doctrine is its after-the-fact nature').

24 See e.g., *McCrady* v. *Oklahoma Department of Public Safety*, 122 P.3d 473, 474–5 (Okla. 2005).

5.48 In jurisdictions that accept the inevitable disclosure doctrine, plaintiffs often try to map the narratives and legal arguments of their case as closely as possible to the influential case in the area, *PepsiCo* v. *Redmond,* in order to increase the likelihood of prevailing. Thus, the focus is on: (1) the intense competition between the former and new employer; (2) the closeness of the former employee's old and new job responsibilities; (3) the high-level position of the former employee; and (4) the time-sensitive nature and competitive value of the alleged trade secrets.

5.49 Fortunately for plaintiffs, the inevitable disclosure doctrine need not be utilized in all cases. Often in the United States it is used as a form of circumstantial evidence to prove the threatened misappropriation that is necessary for the issuance of injunctive relief. Where there is direct or other circumstantial evidence of threatened misappropriation, or evidence of actual misappropriation, the plaintiff in a trade secret case need not argue that the threatened use or disclosure of the information is 'inevitable'. In countries that do not provide relief for threatened misappropriation of trade secrets, the doctrine would be inapplicable because it is unnecessary.

VI. OWNERSHIP AND INVENTION AGREEMENTS

5.50 Usually, the trade secrets of a company will pre-exist the employment of an individual or be the work-product of management or other employees. In such cases, the employees to whom the information is disclosed have no claim of ownership in the information. Sometimes, however, the person who is being accused of trade secret misappropriation claims to be the person who actually created the trade secret (e.g. an employee of the company asserting the trade secret rights). This scenario presents an ownership dispute over the trade secret.

5.51 Neither the UTSA nor Article 39 of the TRIPS Agreement directly addresses the question of trade secret ownership. This is undoubtedly due to the fact that most trade secret cases involve the transfer of information from the putative trade secret owner (like the company-employer) to another (like an employee). However, common law rules have developed in the United States and elsewhere to govern the ownership of employee-created inventions and, by extension, employee-created information. In civil law countries, statutes may exist to govern the ownership of such inventions and information.

5.52 In the absence of an express 'invention assignment agreement' or similar agreement, discussed below, the issue of trade secret ownership in the United States is generally resolved by application of principles that were developed

with respect to disputes concerning patent ownership.[25] The general rule in the United States is that the inventor/creator owns the trade secrets. There are, however, three important and well-established exceptions to the general rule.[26]

5.53 The first way to avoid the general presumption of inventor/creator ownership is to require employees to execute 'invention assignment agreements' transferring all rights and ownership in employee inventions to the employer. These agreements are generally enforceable if they are reasonable. However, some states, like California, have specific statutes that define the acceptable parameters of invention assignment agreements.[27] Also, as with confidentiality and non-compete agreements, invention assignment agreements must ordinarily be supported by consideration and in some countries (discussed in Chapter 7), the required amount of consideration can be considerable.

5.54 Second, if inventing is part of the employee's job, then the employer owns the employee's invention. This is also known as the 'hired to invent' rule. If an invention results from work done by the employee within the scope of her assigned duties, then the employer owns it.[28] The *Restatement of Unfair Competition* (s. 42, comment e), indicates that this rule applies even when the end result is the product of the employee's skill and knowledge.

5.55 The hired to invent concept in the United States, while similar to the 'within the scope of employment' concept of the common law principle of *respondeat superior*, is not usually as broad. Thus, an employee may be working within her scope of employment but not be working within the scope of the inventive activity she was hired to conduct. Also, an employee may be hired to invent one type of invention but actually invent another type of invention. Accordingly, if an employee is not hired to invent and the invention did not result from the employee's assigned work, the employee is likely to own the invention. If, however, the employer's trade secrets were used without authorization in creating the invention, then the employee may be liable to the employer for misappropriation.

5.56 A third exception to the general rule of inventor/creator ownership in the United States is the 'shop right'. This doctrine provides that if the invention was created using resources of the employer (in non-hired to invent situations), then the employer may have a 'shop right' in the invention. The shop right doctrine is

25 See *Banks* v. *Unisys Corp.*, 228 F.3d 1357, 1359 (Fed. Cir. 2000).

26 See *Restatement (Third) of Unfair Competition* (1995), s. 42, comment e; *Restatement (Second) of Agency* (1958), s. 397, comment a.

27 See California Labor Code, ss. 2870–2.

28 See *United States* v. *Dubilier Condenser Corp.*, 289 US 178 (1933).

an equitable doctrine meant to enforce an implied agreement that the employer can use an invention or to provide fair compensation to the employer for its contribution to the invention.[29] In effect, the doctrine allows the employer to share in the invention rather than obtain ownership of it. A weakness of shop rights is that they are not usually transferrable. However, they may arise out of relationships with independent contractors as well as with employees.

VII. EMPLOYEE SELECTION, TRAINING AND OVERSIGHT

5.57 As litigation matters and news reports in the United States and elsewhere establish, trade secrets are at great risk in the workplace. Indeed, statistically, the biggest threat of trade secret misappropriation often comes from employees and other insiders rather than from those external to the company. The lesson for trade secret owners is that they must be vigilant and proactive in maintaining and protecting their trade secrets at all times. In Chapter 4, general advice for establishing and implementing a trade secret protection programme was given. The following provides specific advice with respect to employees.

5.58 A trade secret protection programme with respect to employees should begin with the hiring and in-take process. It is generally recommended that employees who will be given access to trade secrets be thoroughly vetted for honesty and veracity before they are hired and that their activities (particularly their computer usage) be carefully monitored throughout their employment. In this regard, the loyalty and motivations of employees can change over time. Disgruntled employees, in particular, pose threats and corporate security programmes must take steps to address these threats, especially in the days and weeks leading up to an employee's termination. Steps must also be taken during the hiring process to make sure that new employees do not bring the trade secrets of their former employers to their new job.

5.59 As previously discussed, all employees who will be given access to trade secrets should be required to execute an enforceable written confidentiality agreement. But even if such an agreement is obtained, employees need to be educated and reminded about the scope of their obligations of confidentiality. Thus, the periodic training of employees is also recommended, particularly given the fact that the identity of trade secret information can change over time. This is not only important with respect to a company's own trade secrets and proprietary information, but with respect to whatever information of others a company is handling.

---

29 See *ibid.* 188–9.

5.60 A common deficiency of trade secret protection programmes is to have them in name only and to actually handle documents as if no confidentiality obligations apply. This creates an environment in which employees can rightly claim that they did not know or have reason to know which information was to be treated as trade secrets and which information could be used freely. On the other hand, the over-assertion of rights in information can have the effect of lessening the importance of true trade secrets in employees' minds because it seems like all information is treated alike.

5.61 For the foregoing reasons, it is important that companies do not take the position that every bit of information that they utilize in their business is a trade secret. Such a claim fails to put employees on notice of the actual information that can qualify for trade secret protection. Moreover, courts in the United States have shown reluctance to sanction the over-broad assertion of trade secret rights when to do so would limit the mobility of employees. Also, the more information that is identified for protection, the more difficult and costly it will be to manage the trade secret protection programme. Instead, it is generally recommended that companies develop a classification scheme for information that differentiates between trade secrets, other business information and public information.

5.62 Another component of a reasonable trade secret protection programme requires companies to assess the actual threats to trade secrets posed by employees.[30] These threats will then dictate the scope and nature of the required trade secret protection programme. For instance, the strategies that are used to maintain the secrecy of a recipe that only needs to be known by a few people will be different from those that should be used to protect computer code that is embedded in mass-distributed software. The proactive planning and mindfulness of the interaction of employees with company trade secrets is the best approach to avoiding the loss of trade secrecy.

5.63 Computer technology poses a grave threat to the protection of trade secrets in the workplace because it enables easy and surreptitious acquisition and dissemination of trade secret information. The fact that employees have legal access to trade secret information by virtue of their employment can lead to large-scale misappropriation. If not adequately supervised and monitored, employees who have access to a company's computer systems can easily download large amounts of electronic information containing trade secrets on to jump drives or upload it to the Cloud and then transfer that information to competitors. It is not uncommon for employees moving to a new job to take a

30 See Elizabeth A. Rowe, 'A Sociological Approach to Misappropriation' (2009) 58 *U Kan. L Rev.* 1.

wide range of files and other information on which they worked, perhaps intending that such information will be used for reference, or believing that it belongs to them.

5.64 Not only should companies be mindful of protecting trade secrets in the various physical spaces where employees report for work, they should also be cautious about whether and how employees can access and use trade secrets remotely. Consideration should be given to whether some of the technological features of company computers should be disabled for some employees, such as access to Cloud sites and the disabling of USB drive portals. Also, for companies that utilize subcontractors and vendors and that offshore all or parts of their manufacturing processes to foreign companies, care must be taken to ensure that the employees of those companies are subject to duties of confidentiality and other trade secret protection strategies.

5.65 Lastly, no trade secret protection programme with respect to employees is complete unless it includes a process for when employment terminates. Usually, this should include timely efforts to restrict an employee's ongoing access to company information and communication devices. It should also include an exit interview with departing employees to remind them of all applicable obligations (including those imposed by any written agreements) and to secure the return of all company owned information and equipment. Depending upon the level of the employee and the circumstances of departure, the process may also include a search of the employee's work premises and devices, including an examination of any uploading and downloading activities. Often private investigative services and computer forensic experts are utilized for this purpose.

6

ENFORCEMENT MECHANISMS AND LITIGATION

I. INTRODUCTION

6.01 As stressed in Chapters 4 and 5, the best strategy for a business that needs to protect its trade secrets is to develop a trade secret protection programme that includes: instituting adequate security measures; obtaining appropriate confidentiality agreements; and vigilance in monitoring for compliance. However, there may come a time when those measures fail and steps must be taken quickly to preserve the trade secret status of threatened information. Whether this can be done successfully depends upon the enforcement mechanisms that are available in the country where enforcement is sought. Thus, consideration should always be given to the available enforcement mechanisms before any trade secrets are disclosed in a given country. It may be that the benefits of offshoring certain business functions are outweighed by the threats to trade secrets, but this is a calculation that should be made consciously with a full appreciation of the risks and benefits.

6.02 Chapters 9 and 10 provide an overview of the enforcement mechanisms that are available in seven different countries and, more generally, illustrate the range of legal systems and legal processes that exist throughout the world. As a prelude to that discussion, and because US trade secret law is being touted as a model for trade secret harmonization, this chapter highlights the trade secret enforcement

mechanisms of the United States, including the civil, criminal and administrative actions. These approaches, while distinct, can sometimes be used simultaneously; but each approach has particular advantages and disadvantages relative to one another and legal counsel is often in the best position to decide which options might work best in an individual case.

6.03 The most commonly utilized trade secret enforcement option in the United States is a civil cause of action brought in either state or federal courts. Such actions allow the plaintiff to retain a certain level of control that is not available under criminal enforcement avenues. In criminal actions, it is the government (through local or state prosecutors or the US attorney) that maintains control of the matter and exercises prosecutorial discretion to determine if and when a criminal prosecution will be brought. The administrative option of trade secret enforcement is being used more frequently and generally involves customs enforcement and related actions before the US International Trade Commission (ITC). While customs and ITC actions can be quicker and more efficient, they only apply to goods being imported into the United States and the remedies are much narrower.

6.04 In the sections that follow, the three types of enforcement mechanisms available in the United States are discussed in detail. As with this book generally, this information can be used not only to understand US law but to identify the types of issues that should be considered when researching the enforcement mechanisms of other countries.

II. CIVIL TRADE SECRET CLAIMS

6.05 Most civil trade secret claims in the United States are brought in state courts. However, even though (as of mid-2015) there is no US federal law that establishes a civil cause of action for trade secret misappropriation, it is possible under the US Constitution and applicable federal rules of civil procedure for some trade secret claims to be brought in federal court based upon diversity jurisdiction.[1] Whether filed in a state court or a federal court based upon diversity jurisdiction, usually the trade secret law of the state where the action is filed will apply unless choice of law principles require application of another state's (or country's) laws. Because most US states have adopted and follow the Uniform Trade Secrets Act (UTSA), usually the trade secret law that is applied is that described in the UTSA.

1 See US Constitution, art. III, s. 2; 28 USC s. 1332 (2012).

A. Life-cycle of trade secret litigation in the United States

6.06 Under the procedure that is applicable in both state and federal courts in the United States, a trade secret misappropriation claim is initiated by filing a written complaint with the court, paying applicable fees and then properly serving the complaint on the defendant(s) so that he has notice of the claims. This initiates the 'pleading phase' of civil litigation in the United States. During this phase, the defendant can either file an answer to the complaint (admitting or denying the allegations of the complaint and asserting defences) or challenge the sufficiency of the complaint. It is also during the pleading phase that a case which is originally filed in state court can be removed to federal court and where a defendant may assert counterclaims.

6.07 In constructing a defence to a claim of trade secret misappropriation, a defendant should consider challenging various aspects of the plaintiff's case, including: the relationship between the parties; the trade secret status of the information that was allegedly acquired, used or disclosed; plaintiff's standing to sue; the alleged use of the information; and any public policy arguments that mitigate against liability. A common defence argument is that the information that is claimed as a trade secret lost its protected status when it became generally known. For instance, information that is disclosed in a patent cannot be considered confidential or a trade secret. Where a defendant may have reverse engineered or independently developed a product and obtained the alleged trade secret in that manner, he will argue that no misappropriation occurred.

6.08 Usually the pleading phase of the trade secret litigation in the United States runs from 30 to 90 days, but it can be longer in more contentious cases. Also, in trade secret cases this phase of litigation may be lengthened because of the filing of a motion for preliminary relief, requests for expedited discovery and early discovery disputes.

6.09 Because, as discussed in Chapters 3 to 5, it is crucial for a trade secret owner to avoid the public disclosure of its trade secrets, the filing of most trade secret lawsuits in the United States is coupled with a motion by the plaintiff for preliminary relief, usually in the form of a request for a temporary restraining order (discussed in more detail below). In filing such a motion, the plaintiff seeks a prompt order from the court requiring the defendant not to disclose any trade secrets he may possess or, possibly, the return or seizure of such trade secrets. Under applicable procedural rules, although the grant of a temporary restraining order may be quick, it must be followed by a timely hearing on a preliminary injunction (discussed below) which may be preceded by some

expedited discovery. Thus, this phase of trade secret litigation can take months to conclude and can be very expensive and time-consuming.

6.10 Once the pleading and preliminary relief phases of a trade secret case are complete, and assuming that the case has not been dismissed or settled, US litigation enters the 'discovery phase' during which each side in the litigation is allowed to use various procedural devices (including written interrogatories, depositions and subpoenas) to gather evidence that they deem relevant to the case. This phase of litigation can also be very lengthy, contentious and costly, but is viewed by most US lawyers as an essential part of the civil litigation process. This is because, in contrast to the processes of courts in many other countries, it is the responsibility of the parties (through their attorneys) to collect relevant evidence, and not the judge's or a court official's.

6.11 Following the discovery phase, which is usually scheduled to end on a specific date, the parties enter into the 'pretrial phase'. It is during this phase where a variety of pretrial motions, including motions for summary judgment, may be filed. Unless the pretrial phase results in a judgment for either the plaintiff or the defendant, then the case will go to trial. How long it takes to bring a case to trial in the United States depends upon a number of variables, but most state and federal courts place a premium on the prompt resolution of cases, with resolution within one year being the goal in many cases, but two or three years being allowed in more complex cases.

6.12 After the trial phase of a trade secret case in the United States, there is usually a 'post-trial phase' during which a formal judgment and any necessary orders are rendered in writing. This would include the issuance of a written permanent injunction order if the trade secret owner prevails. Once judgment is entered, the losing party has a right to appeal the judgment to an intermediate appellate court and, ultimately, to the highest court of the state where the action was filed (if filed in state court) or the US Supreme Court (if filed in or removed to federal court).

B. Identifying and protecting trade secrets in litigation

6.13 At the onset of any trade secret misappropriation case, it is important that the parties (especially the defence) not overlook a simple (yet complicated) fact: the claim is about misappropriation of a trade secret. It follows, then, that the plaintiff has a duty to identify its trade secrets with specificity. In most US states, this requirement is imposed by case law and pleading rules. (In California, it is a statutory requirement.) What constitutes an adequate identification

of trade secrets depends upon the nature of the trade secrets, the facts of the case and the jurisdiction where the case is being argued.

6.14 One reason for the specificity requirement is to prevent the plaintiff from using trade secret litigation as a means to conduct competitive intelligence through the guise of the civil discovery process. It also serves the due process purpose of letting defendants know the details of the claims against them. However, the duty to identify trade secrets must be balanced against the need to protect trade secrets from public disclosure during the litigation process. Thus, how and when this should occur is an important consideration for the court and the parties.

6.15 Obviously, a plaintiff does not want to fully disclose the alleged trade secrets in the complaint and thereby waive trade secret protection due to the public nature of court filings. On the other hand, principles of due process and the pleading rules of state and federal courts in the United States generally require that the plaintiff allege enough facts to put the defendant on notice of the claims against him.

6.16 As a practical matter, when presenting its case at trial, the plaintiff will have to explain what its trade secrets are as part of its *prima facie* case. When doing so, there is an obvious risk that whatever trade secrets exist will be revealed during the course of the litigation. This is one reason why the decision to file a trade secret misappropriation claim should not be undertaken lightly. It also explains why many plaintiffs are reluctant to identify their trade secrets early in a case and why they will often fight hard to delay the disclosure of any information concerning their alleged secrets.

6.17 The plaintiff's obligation to identify its alleged trade secrets with particularity is not merely a pleading or evidentiary requirement; it is a very practical requirement. Unless the plaintiff can articulate its putative trade secrets in a concrete way, there is no way to test whether the information meets the three requirements for trade secrecy. This is a particular challenge for trade secret owners who claim trade secrecy for broad or vague categories of information and so-called combination trade secrets. By failing to identify their trade secrets, plaintiffs undermine their ability to show that the information is not generally known and has independent economic value. The inability or unwillingness to identify specific trade secrets may also signal that the plaintiff has not taken reasonable precautions to secure the trade secrets.

6.18 In order to facilitate the discovery process in trade secret cases, most courts in the United States will issue protective orders that are designed to protect

plaintiff's information during the pendency of litigation. As explained in Chapter 3, section 5 of the UTSA explicitly requires courts to do so. In theory, this should help to facilitate the timely identification of trade secrets, but unless the court is forceful in requiring the necessary and timely disclosure of details concerning plaintiffs alleged trade secrets (albeit pursuant to a protective order), the early stages of trade secret litigation in the United States can be consumed by costly and time-consuming disagreements regarding the appropriate scope of discovery.

6.19 In each case, the challenge for courts is to figure out how to accommodate the demands of due process (the need of the defendant to know the details of the claims being made against her) while crafting and enforcing an order that is sufficient to protect plaintiff's putative trade secrets. Because severely restrictive protective orders prevent the parties (particularly a defendant in a trade secret case) from accessing materials and engaging in full and complete discussions with counsel, it is important that courts ensure that they are not granted without careful consideration and adequate justification. The parties can assist the courts by working together to craft a stipulated protective order. In some cases, the court will appoint a special master or disinterested expert to hear secret information and report conclusions to the court.

C. Temporary restraining orders and preliminary injunctions

6.20 The filing of a claim for trade secret misappropriation in the US is ordinarily accompanied by a request for a temporary restraining order (TRO), a preliminary injunction (PI) or both. Preliminary relief is meant to preserve the relative positions of the parties and prevent further disclosure or use of the trade secrets until a trial on the merits can be held. Both the UTSA and the *Restatement (Third) of Unfair Competition* contain provisions that allow courts to grant appropriate injunctive relief.[2] Significantly, they permit courts to enjoin both the actual and threatened misappropriation of trade secrets.

6.21 In the United States, the standards for granting preliminary relief, discussed below, are the same for both TROs and PIs; what is different between the two motions are the amount of notice that must be given to the defendant and the length of time that usually precedes the hearing on the motion. A motion for a TRO is usually filed in cases of extreme emergency, which trade secret plaintiffs often claim to be the case with respect to the threatened loss of their trade secrets. Thus, such motions are often heard by a judge in a matter of hours, not days, and sometimes without any notice to the defendant. Because *ex parte*

2 See Uniform Trade Secrets Act, s. 2 (amended 1985); *Restatement (Third) of Unfair Competition* (1995), s. 44.

motions are disfavoured in the United States, courts will usually only grant TROs without notice in cases where the plaintiff can demonstrate that giving notice will result in the destruction of evidence or the flight of one or more of the defendants. Preliminary injunction hearings typically occur after notice to the defendant and are usually scheduled for a date within the first month of the filing of a complaint, although the procedures and schedules of the applicable courts will vary.

6.22 The requirements for preliminary relief are stringent because the moving party seeks relief before a full trial on the merits and often before any discovery has occurred. The factors to be considered in determining whether to grant preliminary relief in a trade secret case are similar to the factors that are applied in tort cases generally.[3] Generally, preliminary injunctive relief will not be granted unless the moving party can establish: (1) a reasonable likelihood of success on the merits of its claim; (2) that it has no adequate remedy at law; and (3) that it will suffer irreparable harm unless preliminary injunctive relief is granted.[4] Courts also examine the potential harms to the parties and to the public.[5] Upon consideration of these factors, when the scales of equity tip in favour of the plaintiff, preliminary relief will be granted.

6.23 If the plaintiff's motion for preliminary relief is granted, the next challenge for litigants and the court is to determine the proper language, scope and duration of the injunction order. Because of the feared loss of trade secrecy, the plaintiff will typically advocate for broad injunctive relief that frequently extends beyond the actual parties to the litigation. For instance, the plaintiff may request that the preliminary injunction apply to all of the defendants and their agents and associates, including their legal counsel and expert witnesses. If the defendant is a company, the plaintiff will often request that the injunction apply to all officers, employees and agents of the company. Fearing the potential consequences for failing to abide by a court order, including contempt proceedings, the defendant will typically argue for an injunction that only applies to the parties to the litigation and their counsel.

6.24 Because the purpose of TROs and PIs is to preserve the status quo until a decision on the merits of the plaintiff's claims, it is usually easier for a plaintiff

3 See *Restatement (Third) of Unfair Competition* (1995), s. 44(2) (listing eight factors to be considered).

4 See *Clorox Co.* v. *S.C. Johnson & Son, Inc.*, 627 F.Supp.2d 954, 970 (ED Wis. 2009) (citation omitted). See also *Sega Entertainments Ltd* v. *Accolade, Inc.*, 977 F.2d 1510, 1517 (9th Cir. 1992) (describing a different formulation of the test which, among other things, examines 'the balance of hardships').

5 See *SI Handling Systems, Inc.* v. *Heisley*, 753 F.2d 1244, 1254 (3d Cir. 1985) (listing a four-factor test for preliminary relief) (citations omitted).

to obtain a prohibitory injunction rather than a mandatory injunction,[6] even though UTSA, section 2(c) specifically authorizes courts 'in appropriate circumstances' to order affirmative acts to protect trade secrets. In trade secret cases, a prohibitory injunction would be worded to prohibit specified individuals from using or disclosing the alleged trade secrets. A mandatory injunction, in contrast, might require the alleged trade secrets to be returned to the plaintiff or deposited with a third party for safe keeping until such time as the trade secret litigation is completed. As a practical matter, because of the reluctance of courts to grant mandatory preliminary injunctions (and the higher burden of proof that may apply), plaintiffs in trade secret misappropriation cases are well advised to word their proposed injunction orders as prohibitory injunctions.

6.25 An issue arises under US law with respect to mandatory injunctions which is related to the privilege against self-incrimination of the Fifth Amendment to the US Constitution. The issue is whether an individual defendant who is preliminarily enjoined to 'return all trade secrets in his possession' can assert the Fifth Amendment privilege against self-incrimination and refuse to comply with the order. Under applicable Fifth Amendment jurisprudence, if compliance with a court order constitutes an admission of any element of a crime (such as the misappropriation of trade secrets or the possession of stolen property), and there is a theoretical possibility of criminal prosecution, then an individual has a Constitutional right to assert the Fifth Amendment privilege and refuse to comply with the order.[7] However, unlike the invocation of the Fifth Amendment privilege against self-incrimination in criminal cases, the assertion of the privilege in civil cases can be used to infer wrongdoing and, therefore, should not be invoked without careful consideration of the consequences.[8] To avoid such issues, plaintiffs in trade secret cases should consider whether a preliminary injunction order addressed to a company and its agents and employees, rather than to specific individuals who might invoke the Fifth Amendment privilege, would be sufficient to protect their interests.

6.26 If a US court is willing to grant preliminary relief in the form of an injunction, applicable rules of civil procedure usually condition the enforcement of the injunction on the posting of security (also known as a bond or a guarantee) that will be sufficient to compensate the defendant in the event that the preliminary relief was improvidently granted.[9] In an attempt to circumvent this statutory

6 See *Tom Doherty Associates. Inc.* v. Saban Entertainment, Inc., 60 F.3d 27, 34 (2d Cir. 1995) (discussing the differences between a mandatory and prohibitory injunction).

7 See *Fisher* v. *United States*, 425 US 391, 407–12 (1976).

8 See *Baxter* v. *Palmigiano*, 425 US 308, 318–19 (1976).

9 See, e.g., Fed. R Civ. P r. 65(c).

requirement, some confidentiality agreements, discussed in Chapters 4 and 5, contain language purporting to waive the requirement of security. Whether these waivers are enforceable will depend upon the views of the applicable court.

D. Permanent injunctive relief

6.27 In the absence of monetary harm (but sometimes in addition to it), the principal remedy for a trade secret plaintiff following a successful decision on the merits of its case is usually permanent injunctive relief. As indicated earlier, pursuant to section 2(a) of the UTSA, such relief may be granted to enjoin actual or threatened trade secret misappropriation. Also, where granted, it is usually granted for as long as the subject trade secrets continue to qualify for trade secret protection and, therefore, while labelled 'permanent', such orders are not indefinite.

6.28 Although different courts in different jurisdictions may have slightly different formulations of the standards for granting permanent injunctive relief, in *eBay, Inc.* v. *MercExchange, LLC,* the US Supreme Court recognized that the following four well-established factors should be examined: (1) whether the plaintiff has suffered an irreparable injury; (2) whether monetary damages are inadequate to compensate for that injury; (3) the balance of hardships between the plaintiff and defendant; and (4) whether the public interest would be disserved by a permanent injunction.[10] These factors differ slightly from the preliminary injunction factors because, whereas a plaintiff on a motion for preliminary injunction must establish 'a likelihood of success on the merits', for a permanent injunction, the plaintiff must establish actual success.

6.29 Plaintiffs who have proven misappropriation, particularly in UTSA jurisdictions, often argue that they are 'automatically' entitled to injunctive relief because such relief is a statutorily prescribed remedy.[11] Whether this argument will work depends upon the law of the applicable state. There is nothing in the language of UTSA, section 2(a) that specifically requires courts to apply 'principles of equity'. However, consistent with the common law origins of US trade secret law, the grant of permanent injunctive relief is ordinarily subject to principles of equity. Moreover, the use of the word 'may' in UTSA, section 2(a) gives courts discretion to grant injunctive relief and, thus, to consider the equities of each case.[12]

---

10 547 US 388, 391 (2006).

11 See e.g., *E.I. DuPont de Nemours & Co.* v. *Kolon Industries, Inc.*, 894 F.Supp.2d 691 (ED Va. 2012).

12 *Ibid.* 706.

6.30 Applicable law and the facts of each case will dictate the equitable factors on which courts focus when deciding whether to grant permanent injunctive relief. Sometimes the focus is on the first two *eBay*-factors listed above. Other times, the balance of the hardship and the public interest factors play greater roles. In cases where there is only an alleged threat of disclosure, injunctive relief is possible but may not be necessary.[13] In this regard, courts will sometimes consider the anticompetitive consequences of injunctive relief and whether consumers would be hurt thereby.

6.31 As with preliminary injunctions, courts are to carefully consider the proper scope and wording of a permanent injunction order.[14] First, injunctions must be sufficiently specific so that the individuals and companies that are subject to them know what they can and cannot do.[15] Second, because of the anticompetitive nature of trade secret injunctions, care must be taken to make sure that they are not overly broad.[16] The nature of permanent injunctive relief can take many forms depending upon the circumstances and the creativity of the plaintiff and the court. Often they are both mandatory and prohibitory, mandating the return of any misappropriated trade secrets and prohibiting the disclosure or use of such secrets. In addition, prohibitory injunctions may range from simple 'use injunctions' to more complex injunctions that attempt to prevent the defendant from enjoying the fruits of the misappropriated trade secrets.

6.32 The duration of a permanent injunction varies depending on the court's view regarding the purpose of injunctive relief in trade secret cases, as well as the current status of the plaintiff's trade secrets. When the grant of injunctive relief is seen as a penalty for wrongdoing, as opposed to a means of preventing a defendant from benefitting from his wrongdoing, injunctions tend to be longer and more permanent. When injunctions are seen as devices that quell competition, they tend to be shorter.

6.33 As a practical matter, the duration of a permanent injunction depends upon the status of the plaintiff's trade secrets at the time the injunction is issued. If the trade secrets are no longer secret at that time, then an injunction is not needed to prevent them from being disclosed to the public, but a limited injunction may

---

13 See *Standard Brands, Inc.* v. *Zumpe*, 264 F.Supp. 254, 269–71 (ED La. 1967) ('[a]bsent disclosure or imminent threat of disclosure, injunctive relief should not be granted'); *Del Monte Fresh Produce Co.* v. *Dole Food Co.*, 148 F.Supp.2d 1326, 1328 (SD Fla. 2001) (noting that California and Florida law require a 'substantial threat of impending injury').

14 See e.g., *General Electric Co.* v. *Sung*, 843 F.Supp. 776 (D Mass 1994).

15 See *Computek Computer and Office Supplies, Inc.* v. *Walton*, 156 SW.3d 217 (Tex. App. 2005).

16 *Ibid.*

be desired to prevent the defendant from benefiting from his wrongdoing. If a plaintiff's trade secrets retain their trade secret status at the time a judgment is about to be entered, then it may be appropriate to grant injunctive relief without a temporal limit, subject to the right of the defendant to apply to the court to terminate the injunction if and when the trade secrets lose their secrecy. Under either scenario, a court may choose to limit the length of the injunction to the time that it would take a person who is skilled in the art to reverse engineer or independently develop the trade secrets, the so-called 'lead-time advantage'.

E. Compensatory and punitive damages

6.34 As the foregoing discussion of permanent injunctive relief suggests, a plaintiff in a trade secret case need not prove actual harm in order to prevail. However, a plaintiff in a trade secret case in the United States cannot recover monetary damages unless it can prove some measure of actual harm. Actual harm is often measured by lost profits, but this is only likely to apply in trade secret cases where the defendant used the plaintiff's trade secrets in competition with the plaintiff and it can be shown that, but for defendant's competition, plaintiff would have made more profits. Actual harm might also be measured by the value of the trade secrets, but this would only apply in cases where trade secrecy was lost due to the defendant's actions, something that is unlikely to happen if the plaintiff was granted preliminary relief and the defendant complied with the court order.

6.35 Due to the nature of trade secret misappropriation claims and the difficulty of proving actual harm using the traditional measure of damages, under the UTSA the allowable measure of compensatory damages is not limited to lost profits. Damages in trade secret cases can include 'actual loss caused by misappropriation and the unjust enrichment [that is] caused by misappropriation that is not taken into account in computing actual loss'.[17] In practice, the traditional measure of damages based upon plaintiff's actual losses is the focus of most trade secret claims, but the unjust enrichment theory will be used in cases where the plaintiff is not engaged in an active business or where the trade secrets were not disclosed, and thereby, destroyed.

6.36 The availability of compensatory damages under the UTSA is not without its limits. As explained in the comments to section 3, '[l]ike injunctive relief, a monetary recovery for trade secret misappropriation is appropriate only for the

17 Uniform Trade Secrets Act, s. 3(a) (amended 1985). As explained in the commentary to the UTSA, '[a]s long as there is no double counting, Section 3(a) adopts the principle of the recent cases allowing recovery of both a complainant's actual losses and a misappropriator's unjust benefit that are caused by misappropriation.'.

period in which information is entitled to protection as a trade secret, plus the additional period, if any, in which a misappropriator retains an advantage over good faith competitors because of misappropriation'. Additionally, the grant of injunctive relief, either preliminary or permanent, will naturally limit the amount of monetary relief that is available.[18]

6.37 If a plaintiff in a trade secret case acts quickly and is successful in preventing the actual use or disclosure of its trade secrets, then there should be no actual harm, no matter how measured. On the other hand, if there is evidence that the defendant used or disclosed the secrets, an award of compensatory damages is possible. The measure of damages for the wrongful disclosure of trade secrets is likely to be the actual and potential value of the secrets to the plaintiff if there had been no disclosure. Evidence of damage due to the wrongful use of trade secrets can be established based upon a number of different measures.[19] Often in US trade secret litigation the award of monetary damages comes down to a battle of damage experts and involves the question whether the experts' testimony is plausible and believable.

6.38 A successful plaintiff in a trade secret case in the United States may also recover punitive damages in some situations. The UTSA specifically allows for the grant of punitive (or exemplary) damages, but only in cases of 'willful and malicious misappropriation' and only in an amount not to exceed twice the amount of compensatory damages.[20] However, when adopting the UTSA, some states either modified or eliminated this cap.[21]

6.39 Willful and malicious behaviour under the UTSA means something more than the knowing bad acts required to prove trade secret misappropriation. Given the competitive setting in which most trade secret cases arise, some courts have made a distinction between 'motivation by malice' and 'motivation by competition'. Under the latter scenario, it is recognized that competition, even aggressive and ruthless competition, is not bad; to justify an award of punitive

18 Uniform Trade Secrets Act, s. 3 comment (amended 1985) ('A claim for actual damages and net profits can be combined with a claim for injunctive relief, but, if both claims are granted, the injunctive relief ordinarily will preclude a monetary award for a period in which the injunction is effective').

19 See e.g., *In re Jonatzke*, 478 BR 846 (Bankr. ED Mich. 2012) (identifying lost profits, erosion of market share, and out-of-pocket expenses as possible measures of damages); *University Computing Co.* v. *Lykes-Youngstown Corp.*, 504 F.2d 518, 536 (5th Cir. 1974) (identifying the plaintiff's lost profits and the 'benefits, profits, and advantages gained by the defendant in the use of the trade secret' as potential measure of damages) (citation omitted); *Roton Barrier, Inc.* v. *Stanley Works*, 79 F.3d 1112 (Fed. Cir. 1996) (awarding plaintiff both lost profits and price erosion damages).

20 Uniform Trade Secrets Act, s. 3(b) (amended 1985).

21 See e.g., NC Gen. Stat. s. 66–154(c) (2011); Mich. Stat. Ann. Ss. 445.1901–1910 (2012); Mo. Rev. Stat. s. 417.457 (2013). Nebraska did not adopt either the damages or attorney's fees provisions of the UTSA. See Neb. Rev. Stat. ss. 87–501–507 (2012).

damages there must be a showing of actual malice.[22] Note that the same evidence that justifies an award of punitive damages in cases under the UTSA may also justify an award of attorney's fees under the UTSA, and *vice versa*.[23] However, courts should take the grant of punitive damages into account in determining whether an award of attorney's fees is also necessary.[24]

F. Reasonable royalties

6.40 Reasonable royalties are not generally a form of compensatory damages under common law, but they are available under the UTSA in two separate and distinct situations. First, where proof of the amount of actual harm or defendant's profits is difficult or impossible, reasonable royalties may be used an as alternative measure of damages.[25] Significantly, there must first be a finding of the defendant's actual use or disclosure of misappropriated trade secrets. Thus, the award of reasonable royalties under this first scenario is not a substitute for proof of actual harm; rather, it is an alternative measure of compensatory damages. This type of reasonable royalty will often be stated as a 'lump-sum', particularly in cases where the subject information lost its trade secret status before the entry of judgment. In cases where the trade secrets continue to exist, the reasonable royalty measure of damages is usually for the period of defendant's wrongful use of the trade secrets. The amount of any reasonable royalty will generally be based upon expert testimony concerning industry norms with respect to the type of information involved.

6.41 The second reasonable royalty scenario under the UTSA concerns rare situations where the grant of injunctive relief (either preliminary or permanent) would ordinarily be called for except for overriding public interest concerns. According to the UTSA, in 'exceptional circumstances'[26] a court may issue an injunction that conditions use of the trade secret upon payment of a reasonable royalty for the period of time for which use could have been prohibited.[27] The public policy interests that may justify the grant of a so-called 'royalty injunction' in lieu of a regular injunction are not well developed or defined in the

22 *Roton Barrier, Inc.*, 79 F.3d, n. 19 above, at 1120–1.

23 See *Vacco Industries, Inc.* v. *Van Den Berg*, 5 Cal. App. 4th 34, 54 (Cal. Ct App. 1992).

24 Uniform Trade Secrets Act, s. 4, comment (amended 1985).

25 *Ibid.* s. 3(a).

26 There is not a lot of case law in the United States on what constitutes 'exceptional circumstances', but it is clear that the provision was based upon a pre-UTSA case in which the court refused to enjoin the use of trade secrets that were needed for the war effort. See Uniform Trade Secrets Act, s. 2(b), comment (citing and explaining *Republic Aviation Corp.* v. *Schenk*, 152 USPQ 830 (NY Sup. Ct 1967)). In *Progressive Products, Inc.* v. *Swartz*, 258 P.3d 969, 979–80 (Kan. 2011), the court noted that '[t]here are no set rules for what constitutes "exceptional circumstances"'. It went on to explain that the analysis requires consideration of equitable issues similar to those considered for injunctive relief, including the public interest.

27 Uniform Trade Secrets Act, s. 2(b) (amended 1985).

United States, but the provision (and its associated comments) represents one place in the UTSA where the public interest is explicitly mentioned.

G. Attorney's fees

6.42 The general rule in civil cases in the United States (the so-called American rule) is that attorney's fees are not available to the prevailing party. Section 4 of the UTSA modifies this rule for trade secret claims by stating that attorney's fees 'may' be awarded to the prevailing party if: (1) a claim of misappropriation is made in bad faith; (2) a motion to terminate an injunction is made or resisted in bad faith; or (3) wilful and malicious misappropriation exists. Whether or not to grant attorney's fees, and how much to award, is within the discretion of the court.[28] An underlying goal of the UTSA's attorney's fees provision is to act as a deterrent to baseless claims.[29] Consistent with this goal, attorney's fees may be awarded to the prevailing party (either the plaintiff or defendant) on a motion to terminate an injunction. This provision was designed to discourage putative trade secret owners from seeking injunctive relief for anticompetitive purposes.

III. ANCILLARY STATE AND FEDERAL CIVIL CLAIMS

6.43 As discussed in Chapter 3, the UTSA includes a provision (section 7) that was intended to preclude plaintiffs in trade secret misappropriation cases from bringing the variety of common law tort claims relating to the alleged misappropriation of business information that existed before the adoption of the UTSA. Such a provision was deemed necessary to create the uniformity that the drafters of the UTSA wanted and to ensure that only information that actually qualifies for trade secret protection would be the subject of tort claims.

6.44 Unfortunately, the true intent of section 7 of the UTSA is not understood or applied in some states and, thus some states will allow a variety of common law causes of action to be asserted, including tort claims for breach of confidence or misappropriation. Moreover, for other reasons, it is possible for a plaintiff in a trade secret misappropriation case to plead a number of related claims along with the principal claim under the UTSA. The most common ancillary claim is

---

28 See e.g., *Real-Time Laboratories, Inc.* v. *Predator Systems, Inc.*, 757 So.2d 634, 638 (Fla. Dist. Ct App. 2000) (noting that the discretion applies even if there is a finding of bad faith).

29 Uniform Trade Secrets Act, s. 4, comment (amended 1985) ('Section 4 allows a court to award reasonable attorney fees to a prevailing party in specified circumstances as a deterrent to specious claims of misappropriation, to specious efforts by a misappropriator to terminate injunctive relief, and to willful and malicious misappropriation').

a claim for breach of contract, usually with respect to confidentiality agreements and non-compete agreements (discussed in Chapters 4 and 5).

6.45 Depending upon the laws of a given jurisdiction, other statutory or common law claims may apply to the facts, particularly if they are designed to prohibit 'bad acts' that are similar to the act of acquiring trade secrets by improper means. For instance, under US federal law a plaintiff may be able to state a civil claim for relief under the Computer Fraud and Abuse Act (discussed below with respect to its criminal provisions) for activity related to hacking into a computer.[30] Or a claim for conversion of property may be available in jurisdictions where trade secrets are considered to be a form of property that can be converted.[31] Given the right set of facts, it may even be possible to bring an ancillary claim for copyright infringement if the bad acts of the defendant involve the reproduction or distribution of copyright protected works of authorship.[32]

6.46 Attorneys who represent trade secret owners in trade secret misappropriation cases, particularly in jurisdictions that do not follow the UTSA, should always consider what, if any, ancillary claims for relief apply given the particular facts of a case. Although the trade secret claims will usually be the focus of the litigation, ancillary causes of action may provide a useful fall-back position. On the other hand, attorneys who represent the defendant in trade secret cases, particularly in UTSA jurisdictions, should argue that the ancillary claims for relief are precluded by section 7 of the UTSA.

IV. CRIMINAL PROSECUTION FOR TRADE SECRET MISAPPROPRIATION

6.47 Some civil wrongs related to intellectual property are also crimes, some are not. For instance, as discussed in Chapter 2, the TRIPS Agreement specifies that countries must adopt laws to make both trademark and copyright counterfeiting a crime. There is no similar provision in TRIPS with respect to trade secret misappropriation, although the various trade secret harmonization efforts and Free Trade Agreements mentioned throughout this book seem determined to change this state of affairs.

6.48 Unlike in the civil context, the United States has both state and federal criminal laws governing trade secrets. However, despite the existence of criminal trade secret laws, criminal actions for trade secret theft are not very common unless

30 18 U.S.C. s. 1030 (2013).

31 See *Hauck Manufacturing Co.* v. *Astec Industries, Inc.*, 375 F.Supp.2d 649, 661 (ED Tenn. 2004).

32 See *M. Bryce and Assocs., Inc.* v. *Gladstone*, 319 N.W.2d 907 (Wis. Ct App. 1982).

they involve an egregious set of facts that will garner the attention of state or federal prosecutors.[33]

6.49 One reason for the paucity of criminal trade secret prosecutions is the fact that state and federal prosecutors are reluctant to use their limited resources to prosecute an economic crime where the victim-company has a readily available, and perhaps better suited, civil cause of action and remedy. Additionally, there are several reasons why a trade secret owner may be disinclined to report a trade secret misappropriation claim to criminal authorities. First, if a report is filed and a criminal prosecution is brought, the trade secret owner effectively loses control of the situation and, in fact, any parallel civil case may be stayed pending resolution of the criminal case. Second, because the trade secret owner lacks control of criminal proceedings, there is a greater risk that its trade secrets will be exposed (and thereby lost) during the criminal proceeding. Third, there is often a public relations concern if news of trade secret misappropriation becomes public, particularly for publicly traded companies that may see their stock price decline.

6.50 Despite the foregoing, criminal prosecutions for trade secret misappropriation can be an effective enforcement tool in some situations. It can be particularly effective where the power of the state (pursuant to a search warrant) is needed to search facilities and seize evidence in a manner that does not require advance notice to the company or individual being searched. In this regard, criminal prosecutions (or at least investigations) are often most valuable with respect to acts of misappropriation that have not yet resulted in the public disclosure of the trade secrets, for instance, where the subject trade secrets involve processes that are used by the misappropriator in secret.

6.51 The following subsections describe a number of applicable criminal laws that exist in the United States at both the state and federal levels and some of the implications of criminal prosecution for trade secret misappropriation.

A. State crimes

6.52 Many states have enacted criminal statutes that are specifically directed at trade secret theft. In states that do not have specific criminal trade secret statutes, other laws which prohibit larceny, property theft or the receipt of stolen

33 See e.g., *Weightman* v. *State*, 975 S.W.2d 621 (Tex. Crim. App. 1998) (affirming conviction of buyer and seller of misappropriated trade secrets related to machine manufacturing industry); *United States* v. *Chung*, 659 F.3d 815 (9th Cir. 2011) (affirming conviction of a former Boeing engineer who provided trade secrets to China).

property may cover trade secret misappropriation, particularly if the alleged trade secrets are embodied in a tangible form.

6.53 Generally, in pursuing a criminal trade secret action prosecutors must prove that the information in question is a trade secret in much the same way as would be required in a civil action (unless the language of the criminal statute suggests otherwise). Accordingly, the same kinds of evidence, such as efforts to preserve secrecy, are required. Unlike civil cases, however, one important additional requirement under the criminal statutes is the *mens rea* (or intent) requirement. Usually, the defendant must have 'knowingly' or 'intentionally' misappropriated the trade secret.[34] This is considered to be a higher standard than the civil requirement under the UTSA that the defendant 'know or have reason to know' that the trade secrets were misappropriated.

6.54 Based upon the foregoing, each criminal statute that may apply to an alleged misappropriation of trade secrets should be carefully evaluated to determine the applicable elements of the crime. With respect to criminal trade secret laws, the definition of a trade secret and whether that definition differs from the UTSA norm is an important consideration. Additionally, the proscribed activity must be identified to determine what acts constitute criminal wrongdoing and what type of *mens rea* must be shown. Not all acts of civil misappropriation are potential crimes.

B. Economic Espionage Act

6.55 To date, the Economic Espionage Act (EEA) is the only federal law on trade secret misappropriation in the United States. Although there have been repeated calls for a federal civil law on trade secret misappropriation (including proposed legislation introduced in 2014), there is currently no civil counterpart to the EEA. Additionally, unlike the Computer Fraud and Abuse Act (discussed below), the EEA does not currently create a private right of action.

6.56 Generally, the EEA gives federal authorities, under the auspices of the US Department of Justice and local federal prosecutors, the power to investigate and prosecute individuals or companies that engage in criminal trade secret misappropriation. Judging from the indictments that have been brought under

34 See e.g., Texas Penal Code Ann. s. 31.05(b) (West 2011) ('A person commits an offense if, without the owner's effective consent, he knowingly' steals, copies, or communicates trade secrets); Colorado Rev. Stat. Ann. s. 18–4-408(1) (West 2013) (requiring 'intent to deprive or withhold from the owner' or 'intent to appropriate … for [the wrongdoer's] own use or the use of another' for the crime of trade secret theft); Alaska Code s. 13A-8–10.4(b) (2013) (requiring that a person 'knowingly' steal, copy, or communicate trade secrets in order for the statute to apply).

the EEA, the vast majority of prosecutions involve employees, former employees and other company 'insiders'. However, acts of corporate espionage by outsiders are also covered by the EEA.

6.57 The prototypical EEA case involves employees who violate their duty of confidentiality or loyalty by using or disclosing their employer's confidential business information. For example, in July 2010, two individuals were indicted for stealing and selling US $40 million worth of trade secret information related to General Motor's hybrid automobile plans.[35] The allegations were that the employees downloaded and saved confidential General Motors documents and then gave the information to a Chinese automaker. This is representative of a large number of EEA prosecutions in which Chinese nationals are over-represented relative to other countries.

6.58 Sections 1831 and 1832 of the EEA define the prohibited conduct under the Act.[36] The criminal wrongdoing can take five basic forms. The statute states that it applies to:

> a. Whoever, intending or … knowingly –
>
> (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;
> (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;
> (3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
> (4) attempts to commit any offense described in any of paragraphs (1) through (3); or
> (5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy.[37]

Thus, it applies not only to the actual acts of misappropriation as defined, but to the acts of 'attempting to' and 'conspiring with others to' engage in one of the listed bad acts.

6.59 The decision of which of the two sections to apply turns on whether the theft was intended to benefit a foreign government. If so, the conduct falls under section 1831. Section 1832, in contrast, is similar to a UTSA claim except that

35 See *United States* v. *Qin*, No. 10–CV–20454 (ED Mich. 2010).
36 18 USC ss. 1831–1832 (2013).
37 18 USC ss. 1831(a), 1832(a) (2013).

it includes additional elements. First, it applies only when there is intent to 'convert a trade secret … related to a product or service used in or intended for use in interstate or foreign commerce'.[38] Second, the actor must intend or know that the conversion will harm the trade secret owner.[39] These requirements are not elements of a civil misappropriation claim and, therefore, are important distinctions between EEA prosecutions and civil misappropriation claims.

6.60 In *United States* v. *Aleynikov*, the court reversed the conviction of the defendant based upon a finding that the subject trade secrets were not 'produced for' or 'placed in' interstate commerce as was then required by section 1832(a).[40] In response to this decision, Congress passed legislation to amend the EEA with the apparent intent to broaden and clarify the wrongful activities to which it applies.[41] This legislation was signed by President Obama on 28 December 2012.

6.61 As amended, section 1832(a) now covers theft of a trade secret 'that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof'.[42] Because this 'in commerce' requirement provides the Constitutional basis for the enactment of the EEA, it is not an element that can or should be ignored by the parties, particularly since trade secrets that are only used internally within a company may not meet the requirement.[43] Plus, it remains to be seen if the amendments to the EEA to fix the *Aleynikov* problem will actually work to clarify the scope of the statute.

6.62 Section 1839 of the EEA defines trade secrets broadly using a variation on the wording of the UTSA. A 'trade secret' is information that 'the owner thereof has taken reasonable measures to keep … secret', and that 'derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public'.[44] Thus, federal government prosecutors must prove three elements: (1) that the information is actually secret because it is neither known to, nor readily ascertainable by, the public; (2) that the owner took reasonable measures to maintain that secrecy; and (3) that independent economic value was derived from that secrecy.[45] The language of section 1839(3) further provides that information is to be protected

38 18 USC s. 1832(a) (2013).
39 *Ibid*.; see also *United States* v. *Howley*, 707 F.3d 575, 580 (6th Cir. 2013).
40 676 F.3d 71, 82 (2d Cir. 2012).
41 See Theft of Trade Secrets Clarification Act of 2012, Pub. L No. 112–236, 126 Stat. 1627 (2012).
42 18 USC s. 1832(a) (2013).
43 See Aleynikov, 676 F.3d 71, n. 40 above.
44 18 USC s. 1839(3) (2013).
45 See *Chung*, 659 F.3d, n. 33 above, at 824–5.

regardless of its form. Thus, information in electronic or intangible form is protected under the EEA.

6.63 The secrecy requirement is part of the EEA's definition of a trade secret, and like the UTSA, is defined by what it is not: secret information is neither known nor readily ascertainable. However, the EEA defines the relevant group, the members of which may not have knowledge of the information, in a slightly different way. It therefore demonstrates how minor differences in the wording of a trade secret statute may broaden or narrow the universe of information it protects.

6.64 In the UTSA, 'trade secret' is defined as that which is 'not … generally known to, and not … readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use'.[46] Under the UTSA, this has been interpreted to include a subpart of the general public, such as members of a particular industry group or technical discipline. In other words, information need not be known by the public at large in order to be generally known under the UTSA. The EEA changes the last clause of the secrecy requirement to read 'by the public'. Whether this difference was intended and is of great significance remains to be determined through case decisions.

6.65 Both sections 1831 and 1832 make an attempt to steal trade secrets and a conspiracy to steal trade secrets a crime.[47] Thus, it is conceivable that someone may be prosecuted under the EEA even though no trade secrets were, in fact, stolen. As one court has explained: 'to find a defendant guilty of conspiracy, the prosecution must prove (1) that an agreement existed, (2) that it had an unlawful purpose, and (3) that the defendant was a voluntary participant'.[48]

6.66 Typically, most cases under section 1832 are charged as an attempt to steal trade secrets. This serves the highly desirable and practical purpose of the government in not having to prove that the information is actually a trade secret. This is also a welcome relief to victim companies that do not want to risk disclosing their trade secrets in the trial process. Rather, the prosecutor must merely establish that the defendant *thought* the information was a trade secret. This can usually be established through circumstantial evidence. It does, however, raise serious concerns about the culpability of the defendant's conduct, particularly in cases where the subject information does not actually qualify for trade secret protection. Presumably, a federal prosecutor would not file such an action

46 Uniform Trade Secrets Act, s. 1(4) (amended 1985).

47 See 18 USC ss. 1831(a)(4)–(5), 1832(a)(4)–(5) (2013).

48 *United States* v. *Martin*, 228 F.3d 1, 10–11 (1st Cir. 2000).

without first being assured that trade secrets do in fact exist, but since trade secrets are fleeting that may not always be the case.

6.67 In order to address the concern that foreign governments and foreign entities are attempting to steal US trade secrets, the reach of the EEA extends outside the boundaries of the United States. If the theft of a trade secret occurs in a foreign country, jurisdiction may be asserted if: (a) the defendant is a US citizen or corporation; or (b) any 'act in furtherance of the offense' was committed within the United States.[49] Accordingly, the EEA, unlike the UTSA, has explicit extra-territorial reach. To date, that provision is not widely used by prosecutors, in effect leaving unaddressed an effective mechanism to assert extra-territorial jurisdiction for trade secret misappropriation that occurs on foreign soil. For more on the extra-territorial reach of US trade secret law, see the discussion on the International Trade Commission, below.[50]

C. Computer Fraud and Abuse Act

6.68 The Computer Fraud and Abuse Act (CFAA) is a US federal law that was adopted before the advent of the commercial use of the Internet to address the problem of computer hacking and does not directly address trade secret misappropriation.[51] Unlike the EEA, however, it includes a private right of action that some plaintiffs have used to turn a state trade secret claim into a federal case. With respect to potential criminal liability, the CFAA makes it a crime for anyone to intentionally access a computer without authorization or exceeding authorization in order to access 'information from any protected computer'.[52] Because the principal wrongdoing as defined by the CFAA is 'accessing a protected computer', its provisions conceptually overlap with the improper acquisition provisions of trade secret law. Thus, if the facts of a trade secret case involve the acquisition of trade secrets that are stored on a computer, the defendant in a civil trade secret case should also be concerned about potential criminal prosecution under the CFAA.

6.69 Whether the defendant's access to the subject computer was unauthorized or exceeded existing authorization is at the heart of a CFAA claim. While CFAA claims are analogous to the improper means requirement for misappropriation under the UTSA, it is unclear whether they mean the same thing and whether the CFAA requirement is broader or narrower than the UTSA. Of particular

49 18 USC s. 1837 (2013).

50 See also Elizabeth A. Rowe and Daniel Mahfood, 'Trade Secrets, Trade and Extraterritoriality' (2014) 66 *Ala. L Rev.* 63.

51 18 USC s. 1030 (2013).

52 18 USC s. 1030(2)(c) (2013).

concern to individuals who regularly use the Internet is whether a violation of ubiquitous 'terms of use agreements' can make some activities 'unauthorized' for purposes of the CFAA. Similar concerns are raised with respect to common provisions of employment agreements and confidentiality agreements that limit computer access.

D. Other federal or state crimes

6.70 In the same way that state and federal law may exist to provide trade secret owners with potential civil causes of action in addition to a claim for trade secret misappropriation under the UTSA (discussed above), other federal or state criminal statutes may exist that outlaw the particular wrongful behaviour of the alleged misappropriator. At the state level, the crimes of theft and burglary have already been mentioned, but criminal statutes related to fraud, extortion and bribery may also apply. At the federal level, possible crimes under the federal wiretap law[53] and the Racketeer Influenced and Corrupt Organizations Act[54] should be considered. As a practical matter, being able to frame the behaviour of the defendant in non-trade secret (and, therefore, non-commercial) terms may convince state and federal prosecutors to pursue the matter.

V. US INTERNATIONAL TRADE COMMISSION AND CUSTOMS ENFORCEMENT

6.71 On the administrative front in the United States, trade secret owners may pursue an action before the US International Trade Commission (ITC) to enforce their trade secret rights by preventing the importation of infringing goods into the United States. This can be especially useful where asserting extra-territorial jurisdiction over a defendant may be difficult or implausible, for instance, in cases where the defendant is physically located outside of the United States.

6.72 The ITC is an independent, quasi-judicial federal agency that is comprised of six Commissioners appointed by the President of the United States. Pursuant to section 337 of the Tariff Act of 1930, the ITC has the power to hear cases concerning the importation of goods into the United States and, when warranted, can issue an order to seal the US border against products that are shown to be 'unlawful' as defined in the statute.[55] This includes 'unfair methods of

53 18 USC s. 2511 (2012).
54 18 USC ss. 1961–1968 (2012).
55 19 USC s. 1337 (2012).

competition and unfair acts in the importation of articles', which has been interpreted to extend to acts of trade secret misappropriation. As discussed above, section 337 has also been interpreted to permit American trade secret owners to redress trade secret misappropriation that has occurred entirely on foreign soil.

6.73 There are several advantages to choosing the ITC instead of a court for a trade secret misappropriation claim. The speed with which investigations are completed is a top factor. Most investigations are completed in about a year, with more complicated cases being completed within 18 months. Furthermore, because ITC proceedings are *in rem* actions, personal jurisdiction over misappropriators is not necessary, thereby eliminating one of the most difficult challenges in bringing a court action against a foreign defendant. Enforcement, at least in the United States, is also easier as an exclusion order issued by the ITC is enforced by the Customs Service at all ports of entry in the United States. The discovery process carries advantages as well, including nationwide service of process for subpoenas for documents and depositions and virtually unlimited discovery.

6.74 A proceeding under section 337 commences with the filing of a complaint.[56] Once filed, the complaint is reviewed, clarified and supplemented upon request by the ITC, and then submitted to the six Commissioners who vote on whether to commence an investigation. Barring 'exceptional circumstances', the Commissioners usually reach a decision within 30 days of filing.[57] If the Commissioners agree to investigate, they assign the case to an Administrative Law Judge (ALJ) who holds a hearing in a manner similar to a trial in a US federal district court.[58]

6.75 When an investigation is ordered, the ITC issues a notice of institution, which is published in the *Federal Register* a few days later.[59] This publication marks the official institution of an investigation.[60] After a hearing, the ALJ issues an initial determination that the Commissioners may review at the discretion of any one Commissioner. The Commissioners' decision is then appealable to the US Court of Appeal for the Federal Circuit.[61]

---

56 Often, the complaint is submitted for informal review by ITC staff prior to its official submission to the Commissioners.

57 19 CFR s. 210.10(a)(1)(i) (2014).

58 19 CFR s. 210.10(a)(1) (2014).

59 19 CFR s. 210.10(b) (2014).

60 *Ibid*.

61 If the ITC finds a violation of s. 337, its final determination is reviewable by the President for consistency with national trade policies. Thomas A. Broughan, III, 'Modernizing § 337's Domestic Industry Requirement for

6.76 Once a complaint is accepted and an investigation commenced, certain procedural differences of ITC actions favour a trade secret owner-complainant. First, the compressed time-frame of a section 337 investigation relative to an action in state or federal court increases the speed with which a trade secret holder can obtain a remedy, while also reducing litigation expenses. Another key factor that works to a complainant's advantage is that, as noted earlier, the ITC's jurisdiction to issue exclusion orders over imported goods that utilize misappropriated trade secrets is nationwide and *in rem*.[62] This feature eliminates the need to establish personal jurisdiction over a respondent. It is particularly useful when addressing foreign misappropriation and avoids the difficultly of collecting monetary judgments against foreign defendants.[63] However, because an order of the ITC only applies to goods that are being imported into the United States, it does not extend to activities and sales that are occurring in other countries or that originate in the United States.

6.77 While the potential relief that a complainant can seek is narrower before the ITC than in a civil trade secret action, the standard for obtaining injunctive relief is less burdensome at the ITC.[64] Whereas injunctions relating to trade secret misappropriation typically require a showing of, *inter alia*, irreparable injury and the lack of an adequate remedy at law, the ITC grants exclusion orders without consideration of the adequacy of a legal remedy. Instead, it only requires a showing of injury sufficient to demonstrate a violation of section 337.[65]

---

the Global Economy' (2009) 19 *Fed. Circuit BJ* 41, 45 n. 30; 19 USC s. 1337(j) (2012). The President has rarely acted on this authority in modern practice.

62 *Sealed Air Corp.* v. *US International Trade Commission*, 645 F.2d 976, 985 (CCPA 1981) ('An exclusion order operates against goods, not parties. Accordingly, that order was not contingent upon a determination of person or "in personam" jurisdiction over a foreign manufacturer. The Tariff Act of 1930 (Act) and its predecessor, the Tariff Act of 1922, were intended to provide an adequate remedy for domestic industries against unfair methods of competition … beyond the in personam jurisdiction of domestic courts'); see also Robert G. Krupka *et al.*, 'Section 337 and the GATT: The Problem or the Solution' (1993) 42 *Am. U L Rev.* 779, 789.

63 Colleen V. Chien, 'Patently Protectionist? An Empirical Analysis of Patent Cases at the International Trade Commission' (2008) 50 *Wm. and Mary L Rev.* 63, 74–5 (2008).

64 *Ibid.* 78–9 nn. 92–8.

65 *In the Matter of Certain Baseband Processor Chips and Chipsets, Transmitter and Receiver (Radio) Chips, Power Control Chips, and Products Containing Same, including Cellular Telephone Handsets*, Investigation No. 337-TA-543 (2011), at 62–3 n. 230, available at www.usitc.gov/publications/337/pub4258vol1of2.pdf. The Commission found that the 1988 amendments to s. 337 eliminating the 'substantial injury' requirement for statutory intellectual property demonstrated Congress' intent to abrogate the traditional equitable requirement of irreparable harm. Although Congress did not eliminate the requirement to show substantial injury with respect to non-statutory intellectual property, like trade secrets, the same reasoning can be applied to argue that Congress did not intend exclusion orders, the sole relief available under s. 337, to depend on any showing beyond those listed in the statute.

6.78 In *TianRui Group* v. *ITC*,[66] the US Court of Appeals for the Federal Circuit held that the Congressional presumption against extra-territorial application of legislation did not apply to section 337 actions for three reasons. First, section 337 is specifically directed to importation of articles into the United States, an inherently international transaction, and thus it is reasonable to assume that Congress intended the statute to apply to conduct that may have occurred abroad. Second, the 'unfair' activity is only prohibited to the extent that it results in importing goods into the United States and causing domestic injury. It does not regulate purely foreign activity. Finally, the court determined that the legislative history of section 337 suggests that Congress intended a broad and flexible reading of the statute.

6.79 From a practical perspective, the *TianRui* approach is far preferable to the lack of a viable means to pursue foreign misappropriators that stems either: (1) from an inability of US litigants to obtain personal jurisdiction over foreign individuals and companies; or (2) from the uncertainty in not knowing which countries' laws will be applied to the dispute. In this regard, under the existing legal framework, the choice-of-law analysis with respect to trade secret misappropriation activities occurring in foreign countries is subject to significant variation. Some courts in the United States treat trade secret misappropriation as a tort for choice-of-law purposes, applying the law of the state where the misappropriation took place. Other courts treat trade secret misappropriation like a breach of contract action and look to the place where the trade secrets were created or where the harm from unlawful disclosure would be realized.

6.80 The *TianRui* approach presents an easier, quicker and more efficient option to trade secret owners dealing with an incident of foreign misappropriation. As between the costs and uncertainty of obtaining jurisdiction through the traditional route or feeling like it is not worth pursuing the alleged infringement at all, the ITC may be an attractive option. Indeed, it may become a new trend. In the past five years, there had been only two completed investigations (including *TianRui*) before the ITC dealing with trade secret misappropriation, and only four cases since 2002. Since the *TianRui* decision in 2011, the ITC has seen an uptick in trade secret misappropriation cases, with five currently listed as pending.[67]

66 661 F.3d 1322 (Fed. Cir. 2011).

67 'All Section 337 Cases', available at http://info.usitc.gov/ouii/public/337inv.nsf/All?OpenView.

7

GOVERNMENT HELD TRADE SECRETS AND DATA EXCLUSIVITY

I. INTRODUCTION

7.01 Federal, state and local governmental entities collect and store large amounts of commercially useful information and data about individuals and businesses. While some of this information is self-generated, some of it is obtained from individuals and companies who are required to file information with the government or who choose to conduct business with the government. This might happen, for instance, where a company submits a bid for a government contract or where an individual files his tax return. It can also occur in industries that are regulated by local, state or federal authorities, such as the banking, pharmaceutical and aviation industries. Although a company may choose not to do business with the government, it cannot choose to avoid applicable regulations and the disclosure of information that is often required by regulators.

7.02 This chapter addresses the legal theories and procedures that can be used to protect business (as opposed to personal) information that is submitted to a governmental entity. Since this book is primarily concerned with trade secret protection, it begins with an examination of the process that should be followed (where possible) to protect trade secrets that are submitted to and held by governmental officials. Next, it examines the separate and distinct topic known as 'data exclusivity' which is the subject of Article 39.3 of the TRIPS Agreement and a focus of the United States Trade Representative's Free Trade Agreement (FTA) strategy. It ends with a discussion of the tension between principles of

government transparency and the protection of trade secrets and other information that is submitted to the government that is often at the heart of complaints about the trade secret protection schemes of various countries.[1]

II. GOVERNMENT HELD TRADE SECRETS

7.03 When companies are required to disclose information to the government, they should be concerned about whether and how their trade secrets and other proprietary information will be protected. As discussed in Chapter 6, this can occur in the course of court proceedings (both civil and criminal), requiring vigilance by trade secret owners to obtain protective orders and to seal court records as necessary. It can also occur as part of regulatory oversight and government contracting, including the marketing approval process that is often a prerequisite to the sale of products and services in a given country. In both settings, principles of open government and the need for transparency concerning the activities of government are often balanced against a business's request for trade secret protection. The reality for trade secret owners operating in a regulated environment is that sometimes the need for public transparency will trump trade secret rights, particularly outside the United States where public interest exceptions appear to be more developed and accepted.

7.04 Wherever a business is operating in the world, it should generally be assumed that information that is submitted to a governmental entity or official will not be kept in confidence and may be used by the government or made available to the public. However, because it is often in the interest of governments to promise a degree of confidentiality and secrecy in order to encourage the submission of needed information or the development of needed products and services, laws and regulations exist to protect specified categories of information. This is true, for instance, in the United States with respect to tax returns and some regulatory filings. It is also often true with respect to public contracts because the inability of governmental officials to promise confidentiality may reduce the number of companies that are willing to bid on government contracts and thereby reduce competition and increase costs.

7.05 No part of the TRIPS Agreement requires WTO member countries to protect trade secrets that are submitted to governmental entities, except for the limited

1 See Elizabeth A. Rowe, 'Striking a Balance: When Should Trade-Secret Law Shield Disclosures to the Government?' (2011) 96 *Iowa L Rev.* 791; David S. Levine, 'The Impact of Trade Secrecy on Public Transparency' in Rochelle C. Dreyfuss and Katherine J. Strandburg (eds), *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research* (2011), p. 406.

obligations of non-disclosure that are specified in Article 39.3 (discussed below). Also, there is no general requirement in the TRIPS Agreement for trade secret owners to be notified and heard before the information that they submit to governmental authorities is disclosed to third parties (although some Free Trade Agreements impose such an obligation with respect to some categories of information).

7.06 Although Article 39.1 of the TRIPS Agreement might be read as a general obligation for WTO members to 'protect undisclosed information', such obligation is directly tied to the obligation under Article 10*bis* of the Paris Convention (1967) to ensure 'effective protection against unfair competition' and usually governmental entities are not competitors. Moreover, when coupled with Article 39.2 of the TRIPS Agreement (which requires what amounts to a private right of action for 'natural and legal persons'), it is clear that the primary concern of TRIPS negotiators was to protect information held by non-governmental entities and individuals.

7.07 Whether the laws of a given country allow a governmental entity to be sued if an official 'wrongfully' acquires, discloses or uses trade secret information submitted to it by an individual or company is a separate issue. Generally, it depends upon two key facts. First, under basic principles of trade secret law (namely, the third party doctrine discussed in Chapter 3), the governmental official or entity must be under an obligation of confidentiality at the time the trade secret information is submitted. Such an obligation may be specified by statute or the applicable government contract, but in many countries (including the United States) it is an exception to the general rule of government openness. Second, under principles of sovereign immunity the governmental official or entity will usually not be subject to suit unless a cause of action is specifically allowed.

7.08 In light of the foregoing, the ability to protect trade secrets in dealings with the government has less to do with available private rights of action and more to do with the obligations of confidentiality and secrecy that governments choose to impose upon themselves. In this regard, Article 1.1 of the TRIPS Agreement states that WTO member countries are free to provide greater protection for intellectual property rights (IPRs) than the TRIPS Agreement requires. This might include legal obligations that are imposed upon governmental officials concerning the confidentiality of certain information.

7.09 In the United States, there is no universal requirement that information that is submitted to the US government must be kept confidential. To the contrary, the presumptive rule (as expressed in state and federal Freedom of Information

Acts) is that information in the hands of the government is open to public disclosure with limited exceptions.[2]

7.10 While there are laws in the United States that make it illegal for governmental employees to disclose information that they acquire in the course of their official duties[3] and trade secret owners can bring what is known as a 'reverse FOIA' action in an attempt to limit governmental disclosures of trade secrets (discussed in more detail below), under US Freedom of Information Act (FOIA) jurisprudence, the decision of whether or not to disclose information is generally within the sound discretion of the governmental officials. Thus, in the same way that there is no absolute guarantee that trade secret information will be kept confidential when it is shared with third parties, there is even less of a guarantee that it will be kept confidential when it is shared with governmental officials.

7.11 Generally, the ability of an information owner to maintain the secrecy of trade secrets and other proprietary information that is submitted to a governmental entity depends upon the applicable laws and regulations or, in the case of government contracts, the applicable bid documents and contracts. It should first be determined if the governmental entity is subject to and follows principles of open government. If so, exceptions to the rule of public access and the steps that must be taken to take advantage of those exceptions should be identified. In the United States, these may be found in the general laws and regulations of local, state and federal governments or in specific regulations and rules of discrete governmental agencies.

7.12 Where exceptions to the principle of open government apply, the information owner is typically required to identify and label the information that it claims to be trade secret or proprietary information, sometimes in very specific ways. The regulations of the US Securities and Exchange Commission (SEC) provide an illustration.[4] These regulations provide for non-disclosure of confidential business information. No specific definition of 'trade secret' (or 'confidential information') appears to be included in the SEC regulations, even though mention is made of trade secrets in a few areas. Rather, the regulations appear to incorporate the FOIA meaning of protected information and a catch-all of 'other reason[s] permitted by Federal law'.

2 See Freedom of Information Act (FOIA), 5 USC s. 552 (2012) and similar state laws.
3 See 18 USC s. 1905 (2012).
4 17 CFR ss. 200.01–.735 (2010).

7.13 The fact that confidential business information comprises a broader group of information, of which trade secrets are a subset, leaves no doubt that the SEC rules would cover trade secrets. Nevertheless, for the SEC to treat information as confidential, the submitter must omit from the material filed that portion that it wishes to remain confidential and must mark the omitted material as 'confidential material' before filing it with the agency. A determination of whether the material will indeed be treated as confidential is not made until a FOIA request has been received for the materials. The regulation lists nine factors that one requesting confidential treatment may address to substantiate the request.[5] Among them are the 'measures taken by the business to protect the confidentiality' of the materials and the 'ease or difficulty of a competitor's obtaining or compiling' the information.

7.14 Based upon the foregoing, when dealing with governmental entities (whether in the United States or elsewhere), it is critical to remember that each one is likely to have its own regulations and practices governing the protection of confidential or trade secret information and there can be wide variation between and among them. The best practice is to determine the applicable regulations and practices and follow them to the letter. However, common sense and the general obligation of 'reasonable efforts to maintain secrecy' play a large part in the process. At a minimum, individuals and companies that do business with the government or that operate in regulated industries are well advised to carefully identify and properly mark all submitted information that they wish to protect from disclosure. Because the categories of information that may be exempt from government disclosure can be different and broader than the definition of a trade secret under applicable law, this may include confidential and proprietary information that would not otherwise qualify for trade secret protection. Where special data exclusivity laws apply (discussed below), it may also include wide swaths of submitted data, such as the data that must accompany applications for US Food and Drug Administration (FDA) approval of new drugs.[6]

7.15 According to annual reports by the US Trade Representative (known as Special 301 Reports), some countries have been criticized for conditioning regulatory and marketing approval on the disclosure of confidential information.[7] In these countries, even the adequate marking of trade secrets may not suffice to protect

---

5 See 17 CFR s. 200.83(d)(2) (2010).

6 See e.g., 21 USC s. 355 (2006). See also e.g., *AstraZeneca Pharmaceutical, LP* v. *FDA*, 872 F.Supp.2d 60 (DDC 2012) (finding no market exclusivity for certain safety information related to the drug Seroquel).

7 See e.g., Office of the US Trade Representative, *2014 Special 301 Report* (2014), p. 31, available at www.ustr.gov/sites/default/files/USTR%202014%20Special%20301%20Report%20to%20Congress%20FINAL.pdf, where China was criticized for 'using regulatory pressure to compel the licensing of technologies'.

information that is submitted to the government, forcing companies that wish to conduct business in those countries to choose between trade secret protection and access to markets. Which choice is made should depend upon the importance of the information claimed to be a trade secret and the value of the potential market. From a practical business standpoint, sometimes the value of a new market exceeds the value of the trade secrets, something that all attorneys should consider when determining how aggressive a trade secret strategy should be.

III. BACKGROUND OF DATA EXCLUSIVITY LAWS

7.16 In addition to including provisions in the TRIPS Agreement to require a minimal level of protection for trade secrets, Article 39.3 of the TRIPS Agreement requires the grant of 'data exclusivity' for certain industries under certain conditions. Because this provision is often misunderstood as being an extension of (or a special circumstance for) trade secret protection, this section discusses the history, purpose, scope and limits of data exclusivity laws.

7.17 By all accounts, the idea of 'data exclusivity' originated in the United States, first in 1972 pursuant to amendments to the Federal Insecticide, Fungicide and Rodenticide Act (FIFRA), and later as a means to solve the 'orphan drug problem' and to facilitate the production of generic drugs.[8] The general idea behind such laws is to encourage certain desired behaviour (such as the sharing of information or the manufacture of needed products) in exchange for a period of data or marketing exclusivity.

7.18 An example of a marketing exclusivity law is the Orphan Drug Act which the US Congress adopted in 1983 as a way to increase the production and marketing of drugs to treat rare diseases.[9] The term 'orphan drug' refers to drugs that have been developed but that are not marketed, often because the costs of regulatory approval (due in part to the tremendous amount of data that must be collected and submitted to establish safety and efficacy) outstrips the market for the drug. This is a particular problem with respect to drugs which cannot qualify for patent protection in the first instance or for which applicable patents have expired. One provision of the Orphan Drug Act grants a seven-year period

8 G. Lee Skillington and Eric M. Solovy, 'The Protection of Test and Other Data Required by Article 39.3 of the TRIPS Agreement' (2003) 24 *Nw J Int'l L and Bus.* 1; Nuno Pires de Carvalho, *The TRIPS Regime of Antitrust and Undisclosed Information* (2008), para. 39.3.3.

9 Pub. L 97–414, 96 Stat. 2049 (1983) (codified in scattered sections of 21 USC, 26 USC and 42 USC).

of market exclusivity to companies that provide the safety and efficacy data needed for the FDA to approve the marketing of the drug.[10]

7.19 Another example of a data exclusivity law (or more accurately, a marketing exclusivity law) concerns the manufacture of drugs by originator and so-called 'generic drug companies' and the costs they must incur when trying to obtain FDA approval for their formulation. To reduce the costs associated with producing generic drugs, the US Congress passed the Drug Price Competition and Patent Term Restoration Act of 1984 (popularly known as the Hatch-Waxman Act) which, in part, allows competitors to utilize the test data and other information first submitted by originator companies to support their own applications for marketing approval.[11] These are known as Abbreviated New Drug Applications (ANDA) which, if granted, come with 180 days of market exclusivity for the first to file.[12]

7.20 In recognition of the costs incurred by originator companies to create and compile the data that is needed for FDA approval, the Hatch-Waxman Act also includes a provision that grants the initial submitter of data a five-year period of market exclusivity for a 'New Molecular Entity' (NME).[13] In practical terms, this means that even if the drug is not protected by a patent, the first company to apply for and receive marketing approval for a NME will enjoy a period of marketing exclusivity.[14]

7.21 Since the United States adopted the Orphan Drug Act and the Hatch-Waxman Act, other countries have taken steps to provide similar data (or marketing) exclusivity. For instance, in 1986, the European Union adopted a Directive similar to the Hatch-Waxman Act.[15] Thus, by the time of the negotiations that led to the TRIPS Agreement, the concept of data exclusivity was well established in both the United States and EU and served as the basis for what became Article 39.3, with the United States being the primary proponent of such a provision. Moreover, the benefits of such laws, particularly in extending or expanding the market exclusivity that comes with patent

10 21 USC ss. 360aa–360ee (2012).

11 Pub. L 98–417 (codified at 21 USC s. 355(j) (2013)).

12 21 USC s. 355(j)(5)(B)(iv) (2013).

13 21 USC ss. 355(c)(3)(E)(ii), (j)(5)(F)(ii) (2013).

14 Paul Burgess and John Lucas, 'Which Generic Drug Would You Want to Use? The Federal Circuit's Interpretation of "Active Ingredient", "Active Moiety" and "Approved Product"' (2005) 87 *J Patent and Trademark Off. Soc'y* 11.

15 See Council Directive 87/21/EEC [1987] OJ L15/36 (later consolidated into Directive 2001/83/EC [2007] OJ L311/67). See also Valerie Junod, 'Drug Marketing Exclusivity under United States and European Union Law' (2004) 59 *Food and Drug LJ* 479.

protection, was not lost on highly regulated industries such as the pharmaceutical and agricultural chemical industries.

IV. ARTICLE 39.3 OF THE TRIPS AGREEMENT

7.22 The position that the United States took in the TRIPS negotiations on the issue of data exclusivity primarily reflected the interests of the pharmaceutical and agricultural chemical industries. Those industries were concerned that any data they submitted to governmental officials for regulatory approval, if publicly available, could be used by others to produce competing products. Also, they did not want their competitors to be able to use the safety and efficacy data they collected as the basis for their own regulatory approval. As a practical matter, if competing companies have to collect their own data (rather than 'bootstrapping' on the data of the originator company), the amount of time it takes to obtain regulatory approval is longer, resulting in a *de facto* period of market exclusivity even in cases where patent protection does not apply.

7.23 While the laws and regulations of various countries may provide for greater data exclusivity rights depending upon the behaviour that a country is trying to encourage, Article 39.3 of the TRIPS Agreement only requires data exclusivity in very specific and narrow situations. It states:

> Members, when requiring, as a condition of approving the marketing of pharmaceutical or of agricultural chemical products which utilize new chemical entities, the submission of undisclosed test or other data, the origination of which involves a considerable effort, shall protect such data against unfair commercial use. In addition, Members shall protect such data against disclosure, except where necessary to protect the public, or unless steps are taken to ensure that the data are protected against unfair commercial use.

The first part of Article 39.3 concerns the obligation of regulatory authorities to protect data from 'unfair commercial use', in other words, use by or on behalf of competitors. The second part concerns the obligations of governmental officials to prevent the disclosure of the subject data.

7.24 To be subject to Article 39.3 of the TRIPS Agreement, data must meet five requirements. First, it must concern pharmaceutical or agricultural chemical products. Second, the data must be submitted as a condition of marketing approval, and not voluntarily. Third, like the provisions of the Hatch-Waxman Act noted above, Article 39.3 only applies to data concerning 'new chemical entities'. Fourth, the data must not have been disclosed previously. Lastly, the origination of the data must have involved 'considerable effort'.

7.25 None of the terms used in Article 39.3 are defined in the TRIPS Agreement, leaving those requirements for interpretation by each WTO member country and, ultimately, the WTO Appellate Body as part of any dispute settlement process. As a practical matter, this means that WTO member countries that are disinclined to grant broad data exclusivity rights have some flexibility to define those terms narrowly without running afoul of the TRIPS Agreement. This explains, in part, why the United States has included heightened data exclusivity obligations in the numerous bilateral and multilateral Free Trade Agreements it has entered with other countries (discussed below); generally, such agreements are used to expand data exclusivity requirements.

7.26 How the phrase 'new chemical entities' is defined is of particular interest to the pharmaceutical and agricultural chemical companies that might rely upon the definition to acquire both *de jure* data exclusivity and *de facto* market exclusivity. Possible definitions of the phrase include: (1) 'novel' in a patent law sense; (2) used for the first time; (3) the subject of regulatory approval for the first time anywhere; or (4) the subject of regulatory approval for the first time in a given country. The latter is the narrower formulation and is favoured by pharmaceutical and agricultural chemical companies because, where applied, it means that the same data that is submitted in one country may have different data exclusivity rights when submitted in conjunction with regulatory approval in another country. A related issue is whether the data must be associated with a patented product to be protected or can relate to unpatented products, with the latter interpretation being favoured by businesses.

7.27 Also undefined are the meanings of the terms 'considerable effort' and 'unfair commercial use'. The broadest meaning of the term 'considerable effort' is any effort without any temporal or monetary threshold. Countries that wish to impose a narrower meaning might require specific evidence of the time and money that was expended to compile the data and only protect compilations of data that exceed stated thresholds.

7.28 Another question that may arise with respect to the interpretation and application of Article 39.3 and related data exclusivity laws is whether the subject data need only be 'confidential' or must meet the definition of a trade secret. The majority view is that the data need not qualify for trade secret protection. While data submitted to governments often includes trade secret information, in theory, it might also include 'confidential' information that does not meet the three requirements of trade secrecy.

7.29 The broadest view of the concept of 'unfair commercial use' as used in Article 39.3, and the one that is asserted by pharmaceutical and agricultural chemical

companies, is that no use of the data is allowed, even to the extent that the data cannot be relied upon by governmental authorities for other purposes. A narrower view is that Article 39.3 only precludes the use of the data by competitors. An even narrower (but less accepted) view asserts that the placement of the data exclusivity provisions of the TRIPS Agreement within Article 39 means that Article 39.3 is tied to the prevention of unfair competition obligations of Article 10*bis* of the Paris Convention (1967) and is only applicable in the case of fraudulent activity. Similarly, some argue that it was only intended to apply to information that qualifies for trade secret protection under Article 39.2.

7.30 Unlike the laws of the United States on which it is based, Article 39.3 does not include any time-frame for protection other than to specify that it is designed to prevent unfair commercial use which, presumably, changes over time. This could be both bad and good for data originators because although the applicable time period may be less than five years, it is possible for them to argue for a greater period of protection. However, during the negotiations leading to the adoption of Article 39.3, it was generally understood that the time period should be measured by the time it would take to recoup the costs of collecting the data (often referred to as 'the lead-time advantage'). For safety and efficacy data, this time period is generally believed to be five years, but may be less or more depending upon the specific data exclusivity laws of each country.

7.31 An important limitation on the scope of the data exclusivity obligation of Article 39.3 is set forth in its last sentence. It specifies two exceptions to the obligation not to disclose submitted information. The first is where the disclosure is required in the 'public interest', but what constitutes the public interest is not specifically defined in Article 39.3 or elsewhere in the TRIPS Agreement. Second, disclosure is allowed if it is coupled with some provision that prevents the 'unfair' use of the information by competitors. Although not explicitly stated, this would typically take the form of a period of market exclusivity. The Hatch-Waxman Act provides an illustration; generic drug companies can obtain access to and use submitted data for purposes of obtaining FDA approval, but the originator of that data is granted a period of data exclusivity.

7.32 Given the flexibilities that are built into Article 39.3, particularly with respect to the interpretation of various terms, there may be significant differences between the data exclusivity laws of various WTO member countries. Some countries, like the United States, may provide data exclusivity for data that is not limited to the pharmaceutical and agricultural chemical industries and for greater periods of time than the five-year period that was discussed during the

TRIPS negotiations. Other countries may provide only a minimal degree of data exclusivity that is based upon a narrow interpretation of Article 39.3. As a practical matter, this means that the data exclusivity laws of each country must be carefully examined to determine how particular data sets are treated by the governmental authorities.

7.33 As summarized by one commentator, while most countries have data exclusivity laws that are designed to protect the subject data from both disclosure and use, a minority of countries only protect pharmaceutical and agricultural chemical data from disclosure.[16] Among countries that protect data from use, there are generally two approaches.[17] The first approach precludes use of the submitted data for a specified period of time. The second approach is to grant the originator company a right of remuneration if its data is used by a follow-on company. The second approach focuses on the costs of compiling data while the first approach creates a period of exclusivity that arguably encourages the compilation of the data in the first instance. The United States prefers the first approach as reflected in its own laws and the Free Trade Agreements that it has entered into with other countries.

V. EFFORTS TO INCREASE DATA EXCLUSIVITY

7.34 The negotiating history of the TRIPS Agreement indicates that various industry groups wanted greater data exclusivity protection than Article 39.3 provides in terms of the scope, length and nature of protection. Also, since the TRIPS Agreement went into effect, disagreements have arisen concerning the meaning of its terms and, consequently, the scope of the data exclusivity obligation.

7.35 The United States (and to a lesser degree the EU) has attempted to resolve the disagreements and expand the scope of data exclusivity obligations through its Free Trade Agreement (FTA) strategy which, on the whole, imposes more obligations on signatory countries to protect and enforce IPRs than is required by the TRIPS Agreement (often referred to as 'TRIPS-plus'). Thus, although the specific data exclusivity laws, regulations and practices of a given country should always be examined, the FTAs that have been entered into by a given country are an additional source for understanding applicable data exclusivity obligations. In fact, in countries where such treaties are self-executing, the FTAs are a direct source of law.

16 Carvalho, n. 8 above, para. 39.3.64.
17 *Ibid*. para. 39.3.

7.36 An example of a Free Trade Agreement that increased the data exclusivity obligations of the signatory countries is the agreement between the United States and Australia that entered into force on 1 January 2005. It includes a provision (Article 17.10) concerning 'Measures related to Certain Regulated Industries'. Expanding upon the data exclusivity obligations of the TRIPS Agreement, it generally requires that the signatory countries provide a five-year period of market exclusivity with respect to safety and efficacy data submitted in conjunction with marketing approval for new pharmaceutical products and ten years with respect to new agricultural chemical products.[18]

7.37 Among other differences between Article 39.3 of the TRIPS Agreement, the United States-Australia FTA does not require that the subject data be compiled at 'considerable expense'. Also, a 'new' product is defined narrowly as: 'one that does not contain a chemical entity that has been previously approved in the Party'.[19] In other words, the definition is not limited to data that is 'novel' in the patent sense, meaning that more data will qualify for data exclusivity than might be the case in other countries. With respect to information that is not 'new' but meets other definitional requirements, Article 17.10.1 of the United States-Australia FTA provides for a five-year period of market exclusivity for pharmaceutical products and a ten-year period of market exclusivity for agricultural chemical products.[20] This is a significant departure from the requirements of the TRIPS Agreement because the United States-Australia FTA provides market exclusivity for a broader set of information.

7.38 United States' FTAs which include provisions that are similar to the United States-Australia FTA (but which may vary slightly in the wording, scope and term of protection) include those entered into between the United States and the following countries: Bahrain (Article 14.9); Chile (Article 17.10); Columbia (Article 16.10); Jordan (Article 4.22–23); Korea (Article 18.9); Morocco (Article 15.10); Oman (Article 15.9); Panama (Article 15.10); Peru (Article 16.10); and Singapore (Article 16.8). The multilateral FTAs between the United States, Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua and the Dominican Republic (referred to as the 'CAFTA-DR FTA') and between the United States, Canada and Mexico (referred to as the 'NAFTA') also include data exclusivity provisions in Article 15.11 and Article 1711(5–7) respectively. Similar provisions are also included in the proposed Trans-Pacific Partnership Agreement (TPP) between the United States, Australia, Brunei Darussalem, Canada, Chile, Japan, Malaysia, Mexico, New

18 See United States-Australia Free Trade Agreement, 18 May 2004, 118 Stat. 919, art. 17.10.1(b), available at www.ustr.gov/trade-agreements/free-trade-agreements/australian-fta/final-text.

19 See *ibid.* Art. 17.10.1(d).

20 *Ibid.* Art. 17.10.1(c)

Zealand, Peru, Singapore and Vietnam, and the proposed Trans-Atlantic Trade and Investment Partnership (TTIP) between the United States and the European Union.[21]

7.39 To date, no United States' FTA has extended data exclusivity obligations beyond the marketing approval for pharmaceutical and agricultural chemical products, but this does not mean that data exclusivity rights do not exist for other products and services in some countries. Thus, if the data that a company seeks to protect does not fall into either of those two categories, other laws and regulations should be examined to determine the extent and nature of applicable data exclusivity rights, if any.

7.40 The European Union has also entered into Free Trade Agreements with various countries throughout the world. These agreements should also be consulted to determine if they require data exclusivity (or IPR protection) that is greater than what is required by the TRIPS Agreement. As of the date of publication of this book, the EU has entered into FTAs with: Chile, Korea, Mexico, South Africa, Canada, India, Malaysia, Singapore and Ukraine. It has also entered into a number of regional FTAs, including the Gulf Cooperation Council (GCC) FTA and the Association of Southeast Asian Nations (ASEAN) FTA.

7.41 The European Free Trade Association (EFTA) (an intergovernmental organization promoting trade for the benefit of its four member states, Switzerland, Ireland, Liechtenstein and Norway) has entered into several FTAs with other countries, most of them touching on data exclusivity only in passing. For example, the agreements between the EFTA and Croatia, Israel, Jordan, Macedonia, Mexico and Morocco only require that the parties maintain 'adequate and effective' protection for undisclosed information.[22] Some other EFTA agreements require an eight-year period of data exclusivity for pharmaceutical products and a ten-year period for agricultural chemical products, but otherwise simply refer to Article 39 of the TRIPS Agreement (for example, the agreements with Albania, Bosnia and Herzegovina, Peru and Serbia).

---

21 See e.g., United States Trade Representative *et al.*, Trans-Pacific Partnership Agreement (TPP), Art. QQ.E.XX.4, 'Protection of Undisclosed Data' (2013), available at www.eff.org/issues/tpp. See also Purported Summary of March 2014 TTIP Negotiations, available at http://keionline.org/node/1984 (noting US concerns about data exclusivity) ('Regulatory test data: the US continues to convey the concerns of some stakeholders regarding the treatment of undisclosed (pharmaceutical) test data; US insistent on clarifying safeguards regarding TRIPS compliance issues and potential negative consequences in the 3rd countries').

22 Rosario G. Cartegena and Amir Attaran, 'A Study of Pharmaceutical Data Exclusivity Laws in Latin America: Is Access to Affordable Medicine Threatened?' (2009) 17 *Health LJ* 269.

VI. GOVERNMENT TRANSPARENCY AND DATA EXCLUSIVITY

7.42 Prior to the advent of data exclusivity laws, the laws of the United States and other countries reflected the importance of government transparency by generally requiring that government records be available for public review. For instance, the US Freedom of Information Act provides that any person has a right to obtain federal government agency records unless those records (or portions thereof) are exempted from public disclosure by certain enumerated exceptions.[23] Similarly, in the EU, citizens and residents have a right to access documents of the 'institutions, bodies, offices and agencies' of the Union.[24] In Japan, the Law concerning Access to Information Held by Administrative Organs provides comparable rights.[25]

7.43 Increased efforts to provide data exclusivity and to protect trade secrets has created a conflict between the values of government transparency and the desire to protect important business information that has yet to be fully resolved.[26] Companies who can reap benefits from data exclusivity rules or who wish to protect their trade secrets will usually fight hard to prevent the disclosure of their information by government officials, even if it means suing the relevant government agency to prevent disclosures. But whether and how such lawsuits can be brought in a given country is the critical question.

7.44 In the United States, lawsuits by companies that wish to prevent the disclosure of their trade secrets or exclusive data are called 'reverse FOIA actions' because they are brought by the information owner rather than by the person or company that is requesting disclosure.[27] Based upon the explicit language of the FOIA, there are applicable exemptions that allow governmental officials to refuse to produce certain categories of business information, but the decision whether to invoke the exemptions is generally within the discretion of the government unless a specific law or a contract between the government and the information owner provides otherwise.[28] Thus, both direct and reverse FOIA actions typically concern the scope and application of applicable exemptions

---

23 5 USC s. 552 (2012).

24 Treaty on the Functioning of the European Union, Art. 15 [2010] OJ C83/47, available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012E/TXT&from=EN.

25 Law concerning Access to Information Held by Administrative Organs, Law No. 42 of 1999, ch. 2 (Japan), available at www.soumu.go.jp/main_sosiki/gyoukan/kanri/translation4.htm.

26 See Rowe, n. 1 above; Levine, n. 1 above.

27 See 5 USC ss. 701–6 (2006); *Mallinckrodt Inc.* v. *West*, 140 F.Supp.2d 1, 4 (DDC 2000).

28 *Chrysler Corp.* v. *Brown*, 441 US 281, 292–4 (1979) (finding FOIA exemptions to be permissive, not mandatory).

and whether the information threatened with disclosure actually qualifies for protection. It is by no means certain that the information will be protected from disclosure.

7.45 Using US law as a benchmark, it is possible that the laws of other countries provide either greater or lesser confidentiality for information submitted to the government, but generally there is always a risk that any information that is submitted to the government will not be kept in confidence. This is particularly true in countries that follow a general policy of government transparency, but the general rule also applies due to exceptions 'in the public interest' which are explicitly allowed by the TRIPS Agreement.

7.46 Similar to US law, in Canada, for instance, when trade secrets or confidential information is disclosed to government agencies, they may be protected,[29] but the rules of each agency must be reviewed on a case-by-case basis to determine the terms and conditions. Also, certain third party disclosures may be permissible or applicable under the Canadian government's freedom of information provisions, and these disclosures could place the trade secret information at risk.[30]

7.47 In Mexico, while the Federal Law on Transparency and Access to Governmental Public Information provides access to information held by the government, article 7 of the IPL excludes information marked confidential from these obligations. Most government agency regulations contain provisions regarding labelling information as confidential. Another provision of Mexican law provides that trade secrets that are disclosed to a government authority are not to be considered part of the public domain and thus can still be considered confidential (article 82 of the Industrial Property Law). Accordingly, the foregoing laws and regulations (and ones like it) should be consulted to ensure, if possible, that trade secret or confidential information is not disclosed when dealing with the government.

7.48 In Brazil, when trade secrets are submitted to government agencies, the agency may be required to maintain their secrecy. Indeed, the unauthorized disclosure, exploitation or use of confidential information submitted by a party to a government agency for the purpose of obtaining approvals required by law is a crime.[31] An exception exists for disclosures aimed at the protection of consumers. It is worth noting, however, that Brazilian law does not protect data

29 Access to Information Act, RSC 1985, c. A-1, s. 20(1).

30 *Ibid.*

31 1996 Industrial Property Law, art. 195(XIV).

submitted for regulatory approval of pharmaceuticals, although it is available for veterinary medicines and agricultural chemicals.

7.49 Ironically, countries like China that are known not to follow a policy of government transparency may provide greater possibilities for the protection of information submitted to the government, but a related concern is that the information will be used by the government itself. The key determining factor is whether the applicable data exclusivity law only prohibits competitors from using the information or whether the government is precluded from using the information as well. Chinese law provides six years of data exclusivity related to new chemical entities but only explicitly precludes use of the data by competitors.[32] The law also contains an exception with respect to the public interest that, it is feared, might be used to allow generic drug manufacturers to use the data.[33]

7.50 To summarize: while protection against the disclosure of data related to regulatory oversight may be available in a given country, the disclosing party should review the applicable legislation and regulations to determine what measures should be taken to preserve confidentiality of the information. As a practical matter, companies that submit information to government regulatory officials should be careful to label their information with appropriate legends that identify the confidential or proprietary information, where allowed to do so. Efforts should also be undertaken, where possible, to obtain an express agreement of confidentiality from the applicable government entity.

32 Regulations for Implementation of the Drug Administration Law of the People's Republic of China, art. 35.

33 See Office of the US Trade Representative, *2013 Special 301 Report* (2013), p. 36.

Part II

OVERVIEW OF TRADE SECRET LAW IN SELECT COUNTRIES

8

UNDERSTANDING THE LAWS OF OTHER COUNTRIES

I. INTRODUCTION

8.01 Part I, Chapter 1 of this book introduced readers to a suggested process and road-map to determine the trade secret laws of other countries that focuses on key issues in trade secret law and various ancillary principles of law. The purpose of Part II is to expand upon that introduction by providing general information about how to determine the laws and procedures of other countries and specific information about the laws of additional countries. This chapter provides the general information. Chapter 9 discusses the trade secret laws of three common law countries (the United Kingdom, Canada and India) and Chapter 10 discusses the trade secret laws of four civil law countries (Brazil, China, Japan and Mexico). Appendix 1 provides a detailed analysis of the proposed EU Trade Secret Directive that, if approved, will dictate the minimum standards for trade secret protection in the European Union.

8.02 In keeping with the content of Part I, the discussion of the laws of specific countries is organized around the following six topics: (1) the general overview of the country's legal system; (2) the general contours of trade secret law, including the definitions of trade secrets and misappropriation; (3) the protection of trade secrets in employment relationships, including issues of trade secret ownership and the use and enforceability of non-disclosure agreements and non-compete agreements; (4) the protection of trade secrets in business-to-business relationships, including the extent to which it is possible to establish an implied duty of confidentiality; (5) potential criminal consequences for trade

secret misappropriation; and (6) various procedural issues related to civil litigation or administrative proceedings to enforce trade secret rights.

8.03 For more detailed and insider information about the laws and legal processes of other countries, it is best to retain an attorney or agent in the subject country, but both the road-map for thinking about trade secret law that is set forth in Chapter 1 and the following information should assist attorneys in understanding the key issues and asking the right questions.

II. DETERMINING THE SOURCES OF LAW

8.04 A key to understanding (or at least navigating) the laws of other countries is to determine the sources of applicable law and their hierarchy within the legal system. Generally, the sources of law can include: written code, case decisions, religious text and custom. It can also include secondary sources, including governmental pronouncements and academic writings. Next, it is important to understand how legal principles are made and the role of judges in that process. Questions to ask include: Are written codes of primary or greater importance than case decisions? If so, what is the effect of case decisions; are they binding or persuasive authority? If case decisions are not binding, then what other sources of information exist to help define the written code? What is the role, if any, of customary law?

8.05 Another key to understanding the laws of other countries is to determine the legal traditions that they follow. As detailed in *The World Factbook* guide to the legal systems of various countries,[1] there are a variety of legal systems operating in the world today. The two major legal systems are the common law system and the civil law system, with the common law system being followed by approximately 80 countries and the civil law system being followed by approximately 150 countries. This explains the countries that are highlighted in Chapters 9 and 10, but it is important to understand that many countries apply aspects of more than one legal tradition, including customary law and religious law. In fact, many countries that were traditionally considered to be common law countries (such as the United States and the United Kingdom) actually have aspects of civil law and, therefore, are hybrid countries.

8.06 The hybrid label can also apply in situations involving the possible existence of different traditions within one country. For instance, while Canada and the United States are primarily common law systems, because of the influence of

1 Available at www.cia.gov/library/publications/the-world-factbook/fields/2100.html.

French settlers the Province of Quebec and the State of Louisiana are primarily civil law jurisdictions. Another hybrid situation is where a civil law country gives some precedential value to case decisions or otherwise has a mixed system of laws. The latter characterization applies to China and the former applies to Brazil and Japan. Although not discussed in this book, other examples of hybrid legal systems include Scotland and the Royal Dutch common law jurisdictions of South Africa and Sri Lanka.

8.07 In keeping with the legal traditions of individual countries, some WTO members (principally civil law countries) have adopted statutes that, at least on paper, provide a high degree of trade secret protection. Other countries, such as India and the United Kingdom, currently rely on the common law of breach of confidence to provide such protection. Still others, like the United States and Japan, have a hybrid system of protection that is part common law and part statutory enactment. This presents a challenge for attorneys and businesses that wish to ascertain what protection is available in each country because (as is the case with each of the US states) it is not enough to just find and read the applicable law; one also must understand how it is interpreted and applied in each individual country.

III. DIFFERENCES BETWEEN CIVIL AND COMMON LAW COUNTRIES

8.08 There are important differences between the legal processes of civil and common law countries with respect to the ways laws are developed, the sources of applicable law and the conduct of litigation, including the pretrial process. The key difference between the two systems is the precedential value (or lack thereof) of case decisions.

8.09 Most countries of the world follow the civil law tradition whereby law is made through the adoption and frequent re-evaluation and amendment of written codes. Historically, civil law countries would first adopt the codes of other (more established) countries, including early Roman law, and then adjust their codes as necessary to meet local conditions and modern needs. Thus, the primary source of law in civil law countries is the written code itself. In contrast, the primary source of law in common law countries is the law as it has developed through case decisions.

8.10 An asserted benefit of the civil law system compared to the common law system is that applicable law is often easier to find because it is compiled into an organized set of written code instead of being dispersed throughout various case decisions. By contrast, in common law countries (except to the extent that the

laws of the country have been codified) it is usually necessary to glean the law from reported case decisions which can be difficult to accomplish if the case decisions are written in a foreign language. For trade secret purposes, however, whether one is in a civil law, a common law or a hybrid jurisdiction, legal research often requires an examination of multiple bodies of law due to the fact that ancillary principles of law, such as competition rules and employment law, are likely to apply in such cases.

8.11 Because the source of civil law is a written code, civil law can be less flexible than common law, but it depends upon how the codes are drafted. Much like the flexibility that is often written into international agreements (including the TRIPS Agreement), codes are often written in general terms to allow for flexibility in application. This can be frustrating for attorneys who are used to common law systems, because how such flexibilities are applied by civil law courts may not be readily apparent and, in any event, will not have binding precedential value. It is important to note, however, that such flexibilities also exist in common law systems with respect to highly fact-specific or equitable elements of a claim, such as the reasonable efforts requirement of trade secret law.

8.12 A hallmark of the common law system is that laws can change and evolve as the facts, circumstances and social norms warrant, meaning that case decisions may become out of date or be explicitly overruled. However, this possibility is moderated by the common law principle of *stare decisis* which generally requires courts to apply the law that was established in earlier cases, thereby preventing wild swings in legal precedent. Unlike the common law, which can evolve slowly over long periods of time, civil codes are frequently re-evaluated and amended as necessary to provide greater clarity or specification.

8.13 Generally, judges in civil law countries rely first and foremost upon a careful reading of the written code and secondarily upon custom. While courts in civil law countries are obviously required to interpret and apply the codes, their decisions usually do not have any binding precedential value, meaning that later courts can see things differently. However, as noted in Chapter 10, some civil law countries have modified this approach and will recognize the decisions of higher courts as binding precedent in some situations. Judges in common law countries, on the other hand, are generally bound to apply court precedent unless it has been overturned by a later case or modified by a statute.

8.14 Another common feature of civil law systems as compared to common law systems is the inquisitorial nature of court proceedings that make the judge the central figure, including as the person who collects and evaluates the relevant

evidence. As a result, pretrial discovery is usually non-existent in civil law countries and, instead, the parties present their respective evidence at the trial (or final hearing) after gathering available internal information and conducting external investigations. Typically, this process is less adversarial than the common law process of adjudication and can be more efficient. It is, however, disconcerting to US lawyers, who are used to engaging in extensive pretrial discovery. This is particularly true in trade secret cases where the nature of the alleged wrong often makes it difficult to collect relevant evidence through the conduct of private investigations.

IV. TREATY OBLIGATIONS AS A SOURCE OF LAW

8.15 When advising a client how to protect trade secrets in a foreign country, one of the first things an attorney should consider is whether the country is a member of the World Trade Organization (WTO) or is a signatory with one or more other countries to any other trade agreements (such as the North American Free Trade Agreement). As explained more fully in Chapter 2, if a country is a member of the WTO, then it is required by Article 39 of the TRIPS Agreement to provide a minimum level of protection for undisclosed information (aka trade secrets). These requirements may be heightened if the subject country is a member of additional multilateral or bilateral trade agreements.

8.16 Whether a country is a member of the WTO can be determined by searching the listing of WTO member countries on the WTO website (www.wto.org). Whether they are a party to other multilateral or bilateral trade agreements that require a heightened form of trade secret protection can be determined by conducting a general search of trade agreements, including the many Free Trade Agreements (FTAs) that have been entered into between other countries and both the United States and the EU. Some of these agreements are referred to in greater detail in Chapter 7. The text of the specific agreements can be found on the website of the United States Trade Representative (USTR) (www.ustr.gov). Similar information is available with respect to the agreements of the European Union (at http://ec.europa.eu/internal_market/index_en.htm).

8.17 Although the various trade agreements are not a substitute for learning the specific laws of a particular country, they provide a useful starting point and preliminary guide to the nature and scope of trade secret protection that member countries are required to implement. This is particularly true in countries where treaties are deemed to be self-executing, meaning that the treaties themselves are a direct source of law.

8.18 In theory, the laws of each WTO member country will be substantially similar with respect to the definition of a trade secret and the meaning of misappropriation because those terms are defined in Article 39.2 of the TRIPS Agreement. However, as with all laws, the actual interpretation and application of Article 39.2 may differ from country to country. As further explained below, this may be due to different social and cultural values or because of differences in the meaning of the same words in different languages.[2] It is also a result of the flexibilities that are contained in the TRIPS Agreement.

8.19 Under the current wording of the TRIPS Agreement, countries have considerable flexibility to determine how best to enforce the trade secret provisions of their laws. For instance, some countries may choose to devote more attention to criminal prosecution than to civil or administrative claims for relief, as is the case with Brazil, discussed below. Thus, a helpful technique for understanding the laws of other countries and how they are applied is to focus on the places in international agreements where flexibility and discretion is allowed. This is often indicated by the terminology 'can or may' instead of 'shall or must'.

8.20 Regardless of the legal traditions of a country, consistent with the general notification obligations of WTO member countries, Article 63.2 of the TRIPS Agreement requires all WTO member countries to regularly report their intellectual property (IP) laws to the WTO. A record of these notifications is kept in a central registry that is maintained by the Secretariat of the WTO and is available for searching online.[3] Copies of many IP laws can also often be found on the website of the World Intellectual Property Organization (WIPO).[4] The Office of the US Trade Representative also gathers information concerning the IP laws of other countries which is often available in various reports, such as the annual *National Trade Estimate Report* and the *Technical Barriers to Trade Report*.[5] In all cases, care must be taken to determine if the listed laws are up to date, particularly with respect to civil law countries, because their process of law-making often results in frequent amendments and updates to applicable law.

---

2 When reading laws that have been translated from their native language into English, keep in mind that nuances in the meaning of the words used in the original may be lost, and thus, the actual interpretation and application of the law of a given country may provide for greater or lesser protection for trade secrets than appears in the translation.

3 See World Trade Organization Search, https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S001.aspx.

4 See WIPO Lex, www.wipo.int/wipolex/en.

5 US Trade Representative, *2014 National Trade Estimate Report on Foreign Trade Barriers* (2014), available at www.ustr.gov/sites/default/files/2014%20NTE%20Report%20on%20FTB.pdf; US Trade Representative, *2014 Report on Technical Barriers to Trade* (2014), available at www.ustr.gov/sites/default/files/2014%20TBT%20Report.pdf.

V. CULTURAL, ECONOMIC AND REGIONAL DIFFERENCES

8.21 Law does not exist in a vacuum but is the by-product of the history, values and norms of a given society. Thus, the meaning and application of the law, whether expressed in written codes or reported case decisions, cannot be determined without due consideration of such matters. For this reason, the discussion of the trade secret laws of various countries that is set forth in Chapters 9 and 10 begins with some background concerning the history and culture of each country. The state of economic development of a country and possible regional differences within a country should also be considered.

8.22 The state of economic development of a country can say a lot about the effectiveness of intellectual property protection in that country. Judging from the history of many countries (including the United States), there is a discernable pattern to the development and enforcement of IP laws that depends in large part on the state of economic development of a country. Generally, where a country is a net importer and user of intellectual property rights (IPRs) (whether in the form of general knowledge, licensed technology or IP protected goods), there tends to be less protection for IPRs. As a country develops its economy, and particularly if it becomes a creator of IP-laden goods and services, it usually becomes more interested in the protection of IPRs because it is motivated to protect the IPRs of its own citizens. In fact, the need to protect the home-grown IPRs of the citizens of the EU is one of the stated reasons behind efforts in the EU to increase trade secret protection, discussed in Appendices 1 and 2.

8.23 Regional differences within a given country, particularly in countries like the United States, Canada, China, Brazil, India and Mexico which have separate states, provinces and territories that may have separate laws and legal principles regarding trade secret enforcement, should also be considered. Moreover, even without different regional laws, the geographic size of a country may cause differences in the application of the law due to the simple fact that the legal norms and values that are developed in one part of a country may not be shared in another part of the country. This is particularly true with respect to large countries like Brazil and China.

VI. PROCEDURAL RULES

8.24 In addition to considering the sources and hierarchy of applicable law for a given country, the procedural processes of each country should be considered. As noted previously with respect to procedure, not all countries have US-style

rules of pleading, discovery or trial. Whereas litigation in common law countries like the United States and the United Kingdom is adversarial, litigation in civil law countries is principally inquisitorial. Civil disputes in these countries are typically heard by a judge or administrative tribunal with no right to a jury trial and little to no pretrial discovery. Also, because the primary source of law in civil law countries is the written code, court decisions tend not to be written or published because they have no precedential value. Instead, official guides or pronouncements and secondary sources (such as the commentary of local lawyers and law review articles) must often be consulted to determine how the laws are actually applied.

8.25 While the TRIPS Agreement includes provisions that require all WTO member countries to provide opportunities for trade secret owners (and IPR owners generally) to enforce their rights, WTO member countries are not required to establish special courts and procedures to enforce trade secret rights.[6] Thus, the real and practical availability of enforcement mechanisms should be a factor that all trade secret owners consider before deciding to share trade secret information with individuals and companies that are located in foreign countries. The sad reality is that some countries, particularly least developed countries, face greater needs (like providing clean drinking water and stopping the spread of Ebola) than establishing efficient judicial systems to enforce the trade secret rights of private companies.

8.26 As a practical matter, consideration should also be given to the timeliness of judicial relief, particularly with respect to the availability of preliminary relief. Not all courts have efficient processes or available resources to consider requests for preliminary relief on an expedited basis or to enforce injunction orders. Thus, although preliminary relief may be available in theory, it is not available in practice.

VII. SECONDARY SOURCES

8.27 In the final analysis, the process of learning the trade secret laws of other countries should involve not only finding dependable descriptions of applicable law and procedure but also acquiring a sense of the extent to which trade secret laws are effectively enforced. Because trade secret rights can easily cease to exist,

6 Agreement on Trade-Related Aspects of Intellectual Property Rights, Art. 41.5, 15 April 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, The Legal Texts: The Results of the Uruguay Round of Multilateral Trade Negotiations (1999), p. 320, 1869 UNTS 299, (1994) 33 ILM 1197 ('TRIPS Agreement').

companies should think carefully about conducting business in countries that do not provide effective and efficient trade secret protection. It may be that the benefits of conducting business in a given country outweigh the potential loss of trade secrets, but if the value of a company's trade secrets outweigh such benefits, then it may be best to avoid doing business in that country. The extent to which a country enforces its trade secret laws may be determined through a review of recent case decisions, but can also be determined by considering secondary sources that relate the experiences of companies doing business in a given country.

8.28 One resource for a rough understanding of the stringency of trade secret laws in various countries is the Trade Secret Protection Index (TSPI) published by the Organisation for Economic Co-operation and Development (OECD).[7] In 2010, researchers commissioned by the OECD conducted a review of the trade secret laws of various countries. Based upon their judgment of the pros and cons of various features of trade secret law (apparently a UTSA-plus conception), the trade secret laws of the countries they studied were ranked using a five factor test.

8.29 Of the 38 countries listed in the 2010 TSPI (as updated in August 2014 to reflect more countries), the United States scored the highest with a score of 4.5 out of 5, followed closely by Canada and Japan. This means that these countries have been deemed by the creators of the Index to have the most stringent trade secret laws, although the creators caution that the Index was not intended to make any normative judgements. In this regard, some of the factors that were ranked low related to the application of principles of free competition and employee mobility which many countries highly value, as discussed below. Apparently, the United States (the country with arguably the most well-developed trade secret law in the world) did not receive a perfect score because many US states place great value on free competition and employee mobility and because misappropriation (wrongfulness) is an essential element of a claim under the Uniform Trade Secrets Act. Based upon a variety of factors, the countries of India, China, Russia, Indonesia and the Philippines had the five lowest ranked systems, with scores of less than 3 out of 5.

8.30 Reports by the USTR and other entities (such as industry groups and IP organizations) regarding the implementation (or lack thereof) of applicable

7 OECD, *Protection of Trade Secrets*, updated 1 August 2014, Rev. 1 available at www.oecd.org/trade/tradedev/OECD-tad-protection-of-trade-secrets-web-annotation.pdf.

trade agreements often provide insights about the details and enforcement of specific laws that should be taken into account by trade secret owners when assessing the risks posed to their important information.

9

COUNTRY OVERVIEWS: COMMON LAW COUNTRIES

I. INTRODUCTION TO COMMON LAW COUNTRIES

9.01 As noted in Chapter 8, there are a number of different legal traditions throughout the world, but the two predominant systems are the common law system and the civil law system. Today, approximately 80 countries follow the common law tradition, including the United States (discussed in Part I).

9.02 For purposes of trade secret law, we begin with a discussion of the common law because, as discussed in Part I, US trade secret law sprang from the common law development of trade secret principles in England beginning in the early 1800s and, thus, it is important to understand how such law has developed since that time. Generally, whereas the United States decided to speed-up and clarify the common law development of trade secret principles by enacting the Uniform Trade Secrets Act, the trade secret laws of the countries featured herein have evolved over a long period of time as part of the common law tort of breach of confidence.

9.03 Three traditional common law countries are discussed in this section: the United Kingdom, Canada and India. However, while the focus of this section is on only three countries, many other common law countries with former ties to Great Britain tend to cite to English court decisions and, thus, the trade secret laws of those countries are very similar to what is discussed below. Also, with respect to the United Kingdom, due to the different legal histories and traditions of the four countries that comprise the UK (England, Wales, Scotland and Northern Ireland), the focus of the following discussion is actually on the law of England and Wales, with some reference to aspects of Scottish law. Similarly, because the Canadian Province of Québec follows the civil law tradition, the following discussion of Canadian law primarily reflects the common law tradition of the other provinces and territories.

9.04 As further explained below, the laws of each of the featured countries share a common heritage owing to the fact that they follow the common law tradition that was first developed in England during the Middle Ages and which subsequently spread across the world, primarily to former colonies of the British Empire. However, in keeping with the common law process, the principles governing breach of confidence in such countries may have diverged in some respects.

9.05 As previously outlined in Chapter 8, the principal feature of the common law tradition is the way legal principles are developed. In a purely common law system, laws are not codified in a code (or statute or regulation) but are developed through judicial decisions which have precedential value, with the decisions of higher appellate courts taking precedence over the decisions of lower appellate courts. Because the common law is not written down (except in reported case decisions), it is thought to be more flexible than civil law, both in terms of the application of common law principles and the ability of the law to adapt and evolve. This is particularly true with respect to cases that are brought 'in equity' as opposed to 'at law', as courts sitting in equity generally have more flexibility to fashion appropriate remedies. However, the flexibility of the common law often frustrates businesses who desire more predictability and clarity. It also makes it more difficult to discern the law, particularly if case decisions are not readily available in an attorney's native language.

9.06 As a practical matter, the common law process means that a primary source of law is judicial decisions and that each successive judicial decision is developed in light of decisions that came before it. Generally, it also means that new legal principles cannot be developed until a case that raises a particular issue is brought before a court and, thus, it can take years for the law to evolve to meet contemporary needs. Typically, case decisions are available in the form of

written opinions that are gathered into collections or reports and, as is the case in the United States, they may also be synthesized and analyzed in treatises. However, the primary source of law remains the case law itself.

9.07 Because the primary source of law in a common law country is case decisions, where the common law of a country is not yet developed on a particular issue, common law courts often look to the non-binding case decisions of other states or provinces (as in the case of the United States and Canada, respectively) or countries for guidance. For instance, the courts in Australia, Canada and New Zealand have all relied upon and cited English breach of confidence cases and the courts of Canada and India have cited trade secret decisions from the United States. For lawyers who are familiar with the common law of one country but who are trying to enforce trade secret rights in another country, this practice can be a helpful tool, particularly since the common law process depends upon lawyers to advocate for changes and additions to existing legal principles.

9.08 In reality, many countries that follow the common law tradition are actually hybrid systems because they have adopted statutes and regulations to govern various aspects of their society (particularly in the areas of criminal and procedural law). The value of statutes and regulations in common law countries is that they can be used to address legal issues before common law principles have time to develop. However, even with respect to written codes and regulations, the precedential value of case decisions that interpret and apply those laws remains paramount in common law countries.

II. UNITED KINGDOM

A. Overview of the legal system

9.09 It is appropriate that the overview of the trade secret laws of various countries begins with a discussion of the law of the United Kingdom. This is because it is generally believed that modern trade secret law (at least in the West) began in England through the common law development of legal principles designed to resolve disputes between competing businesses over the use of secret formulas and processes. It is also because of the influence that England's common law of breach of confidence has had (and continues to have) on the law of other common law countries, including Australia, Canada, India, Ireland and New Zealand.

9.10 Although Americans tend to view the United Kingdom as a unitary government with a unitary legal system and set of laws and a unitary culture, the reality is more complicated, as recent efforts by Scotland to secede from the UK illustrate. In fact, the United Kingdom is the union of four separate countries with three different legal systems and four different legislative bodies (and possibly a fifth if England is allowed to create one). For reasons that will be explained, however, the law governing trade secrets (actually a broader category of information known as 'confidential information') is fairly consistent throughout the UK due to the fact that the Supreme Court is the highest appellate court for all courts in the UK with respect to civil matters. However, particularly since Scotland follows a hybrid system of laws that includes 'Scots Law', some differences in the application of the general principles described herein may apply in each of the four countries of the United Kingdom. For this reason, the discussion of law and procedure that follows is more accurately labelled as the law of England and Wales unless otherwise noted.

9.11 The individual countries that now comprise the UK (England, Northern Ireland, Scotland and Wales) have a centuries-old history, but the history of the United Kingdom began in 1707 with the Treaty of Union which created a political union of the Kingdoms of Scotland and England (including Wales). The Kingdom of Ireland was added to the Union in 1800, with the new unified country being known as the United Kingdom of Great Britain and Ireland. In 1922, Ireland (not including Northern Ireland) split off to form the Irish Free State, later becoming the Republic of Ireland. Thus, since 1922, the UK has been formally known as the United Kingdom of Great Britain and Northern Ireland.

9.12 The United Kingdom is a constitutional monarchy with the Queen (or King) as the Head of State and the Prime Minister as the head of the government. The primary legislative body in the UK for matters of concern to the UK as a whole is the Parliament which consists of the House of Lords and the House of Commons. However, since 1999 some legislative powers have been shared with the Scottish Parliament and the Welsh Assembly. Additionally, pursuant to the Northern Ireland Act 1998 (passed as a result of the Good Friday Agreement), the Northern Ireland Assembly was given some legislative authority which it has been allowed to exercise for most of the twenty-first century.

9.13 Unlike the US system of federalism, where most legislative power is retained by the states with the federal government having only limited powers as defined by the US Constitution, in the United Kingdom the Parliament has the primary legislative power, with the legislative bodies of Northern Ireland, Scotland and Wales having only limited legislative powers as defined by the various 'acts of

devolution' that created those entities. Currently, those powers do not specifically include the enactment of trade secret laws but may apply to the various ancillary areas of law that are often implicated in trade secret cases, including employment law, criminal law and rules of civil procedure. For instance, the enactment of employment law is reserved by the Scottish Parliament. Thus, to understand the law of the UK requires careful consideration of the legislative powers of the various legislative bodies and the laws and procedures adopted and used by each.

9.14 Pursuant to the Treaty of Union, although the previous Parliaments of Scotland and England were merged into one, Scottish and English law remain separate. The legal system of England and Wales is largely based upon English common law and equity. Scottish law (or Scots Law), in contrast, is a hybrid system based in part on common law, ancient Celtic and Pict customs and Norman Feudalism and, since the fifteenth century, the civil law principles of continental Europe. Like England and Wales, the legal system of Northern Ireland is largely based upon common law but with different legal precedents and legal procedures. As is now the case with most common law countries, some laws have been adopted by the UK Parliament or by the legislative bodies of the individual countries.

9.15 The practical effect of the three separate legal traditions in the United Kingdom is that, while country-wide laws may be adopted by the UK Parliament, regional laws do exist and differences in both the substance and application of those laws can result. The discussion that follows focuses on the general principles of trade secret law applicable in England and Wales (mainly based upon the common law development of those principles). While the legal principles of England and Wales are often followed in Northern Ireland and Scotland, unless and until the UK Parliament adopts a UK-wide law that conforms to the proposed EU Trade Secret Directive (see Appendices 1 and 2), the specific laws and legal principles of Northern Ireland and Scotland should be researched as appropriate to determine if and how they diverge from those of England and Wales.

9.16 Because the United Kingdom does not have a unified legal system, it does not have a unified court system either. The court system in England and Wales is similar to the tri-level system of the United States, with lower courts where civil actions are initiated (known as county courts for lower value cases and the 'High Court' for higher value cases), an intermediate appellate court known as a Court of Appeal and the UK Supreme Court (previously a function of the House of Lords). In Northern Ireland there are county courts and the Court of Judicature (consisting of the Crown Court, the High Court of Justice and the Court of Appeal). The county courts are the principal civil courts, but higher

valued cases will be initiated in the High Court. Cases originating in Northern Ireland can ultimately be appealed to the UK Supreme Court. The UK Supreme Court is also the highest court in Scotland, except for criminal cases not involving a Human Rights Act 1998 violation which can be appealed to the Scottish High Court of Justiciary. The lower civil courts of Scotland are the Court of Session and the Sheriff Court, with the Court of Session acting as both a court of first instance and as an appellate court.

9.17 In addition to the common law and statutes as adopted by the various legislative bodies, two other sources of law play a large role in the legal systems of the United Kingdom: European Union law and the European Convention on Human Rights (ECHR).[1] The United Kingdom became a member of the European Union (then known as the European Economic Community) on 1 January 1973 and ratified the ECHR in 1951. Pursuant to the Human Rights Act 1998, which came into force in October 2000, the ECHR was directly incorporated into UK law and became enforceable by UK courts (previously it was only enforceable pursuant to a petition filed with the European Court of Human Rights).

9.18 The United Kingdom does not have a written constitution with a Bill of Rights similar to the US Constitution, but with the codification of the ECHR into UK law, the judicial authorities of the UK are required to protect the rights described therein. Significantly with respect to the scope and enforcement of trade secret rights, this includes: (1) the right to a fair trial (Article 6); the right to freedom of expression (Article 10); and the right to freedom of assembly and association (Article 11).

9.19 The United Kingdom has been a member of the WTO Agreement, and therefore subject to the provisions of the TRIPS Agreement, since its inception on 1 January 1995. As a consequence of its membership in the European Union, it is also a member of the EU negotiating group (formerly referred to as the European Communities (EC) negotiating group) which was an active participant in the Negotiating Group 11 (NG11) negotiations that led to the TRIPS Agreement. Additionally, the UK was an early member of both the Berne Convention (original member since 1886) and the Paris Convention (since 1884).

1 Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950, ETS No. 5; 213 UNTS 221 (ECHR).

B. Contours of trade secret protection

9.20 Due to their longstanding and rich history as common law countries, the trade secret law of the England and Wales is principally defined by the common law as originating in England, beginning with *Newbery* v. *James* in 1817.[2] The essence of the claim is an alleged breach of confidence with respect to confidential information that was shared under circumstances where an obligation of confidentiality is found to exist.[3] Thus, it is similar to the breach of confidence prong of US trade secret law, the key predicate fact being the existence of either an express or implied (in-fact or at-law) duty of confidence.

9.21 Unlike US trade secret law that focuses solely on the protection of qualifying trade secrets, trade secret law in England and Wales is part of the broader law of breach of confidence which also addresses privacy concerns and rights of publicity, among other potential claims.[4] Except in Scotland where the courts are considered to be courts of law and not equity, breach of confidence claims in the United Kingdom are often viewed as equitable in nature, being based upon principles of unfair competition rather than property rights. Accordingly, a court hearing such a claim will often exercise flexibility to do what is deemed right and fair to remedy the situation. However, plaintiffs in breach of confidence cases may also base their claims upon a breach of contract, for instance, a written or oral confidentiality agreement, in which case contract remedies may apply.

9.22 As explained in the leading case, and consistent with the breach of confidentiality prong of US trade secret law, a duty of confidence can arise in two ways under the law of England and Wales: (1) pursuant to an express confidentiality agreement (written or oral); or (2) as a result of circumstances justifying a finding of an implied duty of confidentiality.[5] Two other requirements must also be met to prove a case of breach of confidence. First, the subject information must constitute confidential information and, second, it must be shown that the defendant used or disclosed the information improperly. In a later case, the court added the requirement that the information 'must be information used in a trade or business'.[6]

---

2 35 Eng. Rep. 1011, 1013 (Ct Ch. 1817). See also *Yovatt* v. *Winyard* (1820) 1 Jac. & W 394.

3 See Jon Lang, 'The Protection of Commercial Trade Secrets' (2003) 10 *EIPR* 462.

4 See generally, Megan Richardson, Michael Bryan, Martin Vranken and Katy Barnett, *Breach of Confidence: Social Origins and Modern Developments* (Edward Elgar, 2012).

5 *Coco* v. *A.N. Clark (Engineers) Ltd* [1969] RPC 41.

6 *Lansing Linde Ltd* v. *Kerr* [1991] 1 WLR 251.

9.23 Because the applicable legal principles protect 'confidential information', it provides protection for a conceptually broader set of information than just 'trade secrets' as defined in the Uniform Trade Secrets Act (UTSA) and in Article 39.2 of the TRIPS Agreement. Consistent with US trade secret law, however, this can include both technical trade secrets and non-technical business information. Moreover, while the information that is the subject of a breach of confidence action in England and Wales is often commercial information, a breach of confidence claim can apply to the personal information of individuals. The later claim arises out of the United Kingdom's commitment to enforce the ECHR which requires the protection of personal privacy.[7] Thus, care should be exercised not to confuse the law of the UK as it applies to the protection of personal information with the law that applies to the protection of business information since there can be important differences.

9.24 Consistent with US law (particularly before the adoption of the UTSA), the business information that can be the subject of a breach of confidence claim in England and Wales must be sufficiently secret, although this is a flexible requirement since there is currently no UK statute that defines a trade secret. Rather, consistent with the law that existed in the United States before the adoption of the UTSA, what constitutes a trade secret is an amorphous concept that depends upon the specific facts of each case.

9.25 After the claimant adequately identifies its alleged trade secrets, the courts in England and Wales will examine the nature of the information to determine whether it is confidential or if it has been disclosed to the public (similar to the secrecy element of US law and TRIPS Article 39.2).[8] They will also examine a number of factors to determine if the information is worth protecting, including the extent to which the information owner engaged in efforts to keep the information confidential (similar to the reasonable efforts requirement of US law and TRIPS Article 39.2).[9] Generally, as long as the information has remained relatively secret (i.e. only disclosed to people who are under a duty of confidence), it is confidential information.

9.26 Consistent with the discussion of the nominal novelty requirement of US law in Chapter 3, although novelty in the patent sense is not required for the protection of confidential information in England and Wales, courts are sensitive to the fact that the information that is sought to be protected, even if it is not in the public domain, may not be worth protecting. Thus, trivial, ordinary

---

7 ECHR, art. 8(1), (2).

8 See e.g., *Mustad* v. *Allcock and Dosen* [1963] 3 All ER 416 (involving information disclosed in an issued patent).

9 See e.g., *Cray Valley* [2003] EWHC 728 (citing the UTSA); *Ansell Rubber Co. Pty Ltd* v. *Allied Rubber Industries Pty Ltd* [1967] VR 37; *Dais Studio Pty Ltd* v. *Bullet Creative Pty Ltd* (2007) 165 FCR 92, 116–26 (Jessup J).

or low value information will not be protected.[10] Among other things, this line of cases helps to prevent unmeritorious claims by individuals who submit unsolicited ideas to companies.

9.27 Because breach of confidence law in the England and Wales is similar to the legal principles that existed in the United States before the widespread adoption of the UTSA (many of which still apply in the non-UTSA states of New York and Massachusetts), the focus of the claims is on the alleged wrongful *use* or *disclosure* of the confidential information in breach of a duty of confidence and not upon the wrongful *acquisition* of such information by improper means. In other words, the concept of misappropriation by 'improper means' is not a part of English common law owing to the fact that a breach of confidence claim requires a finding of a duty of confidence. In the appropriate case, however, it may be possible to argue that the improper actions of a wrongful acquirer created an implied duty of confidentiality that was breached by a subsequent use or disclosure of the information. Additionally, other legal theories of liability may apply with respect to specific types of wrongful acquisition, such as computer hacking.

9.28 In Chapter 3, it was explained that one of the refinements that the UTSA made to the common law of trade secrecy was to broaden the definition of improper means to include wrongful behaviour other than a breach of confidence, including acquisition by theft, bribery and espionage. In the absence of legislation like the UTSA, recognition of such a wrongful acquisition claim in England and Wales must either be developed as part of the common law of breach of confidence or be found in another tort theory. There may be some movement in this regard as evidenced by *Tchenguiz* v. *Imerman*,[11] in which the wife in a divorce proceeding was found to have wrongfully acquired confidential information from her husband.

9.29 Because breach of confidence law in England and Wales is a matter of common law and not statute, any limitations that are imposed upon duties of confidence are also a matter of common law. Consistent with US law, one limitation that is clearly established is that reverse engineering is a proper means of acquiring trade secrets and does not constitute a breach of confidence.[12]

---

10 *Attorney-General* v. *Guardian (No. 2)* [1990] 1 A.C. 109, per Lord Goff; *De Maudsley* v. *Palumbo* [1996] FSR 447.

11 [2010] EWCA Civ 908 (finding that a breach of confidence had taken place where plaintiff's former brothers in law accessed his servers in a shared office and turned over confidential files to plaintiff's former spouse during divorce proceeding).

12 *Mars* v. *Tecnowledge* [2000] FSR 138.

9.30 In contrast to the United States, which does not have a well-articulated and cohesive public interest exception to trade secret misappropriation, such an exception has been repeatedly recognized in England since 1856. In the seminal case of *Gartside* v. *Outram*, for instance, the court recognized that an alleged duty of confidence should not be available to hide the commission of a fraud.[13] This public interest exception has since been extended to apply in a number of situations where the public interest was deemed to outweigh the need for confidentiality.[14] This may include the free speech interests guaranteed by Article 10 of the ECHR or national security and public safety interests.

C. Trade secrets in employment relationships

9.31 On the whole, the law governing trade secrets in employment relationships in the United Kingdom is very similar to US law except that the law governing the enforceability of non-compete agreements in the UK seems to tip more in favour of employees than employers. Generally, under applicable law the parties to an employment relationship owe an implied duty of trust toward one another, thereby giving rise to an employee's duty of confidence. Thus, it is not necessary in England and Wales for employers to obtain express confidentiality agreements from their employees in order to have a potential breach of confidence claim. For the reasons that are discussed in Chapter 5, however, it is still highly recommended if for no other reason than to inform employees of the duty of confidence and to avoid any arguments about the scope of that duty.

9.32 The influential case of *Faccenda Chicken* v. *Fowler*[15] provides guidance on the categories of information to which an employee may be exposed and the appropriate lawful use of such information both during and after employment. In so doing, it delineates the types of information that cannot be the subject of a breach of confidence claim in England and Wales and, at least in the employment context, appears to distinguish between confidential business information and technical trade secrets. It also recognizes that it is a breach of an employee's duty of confidence for an employee to memorize confidential information for the purpose of later use.

9.33 The court in *Faccenda Chicken* first reaffirmed the basic principle that publicly available information cannot be the subject of a breach of confidence claim. Thus, employees in the UK are free to use information that is easily accessible

13 (1856) 26 LJ Ch. 113.

14 See e.g., *Initial Services* v. *Putterill* [1968] 1 QB 396, 405; *Attorney-General* v. *Guardian (No. 2)* [1990] 1 AC 109, 282; *Beloff* v. *Pressdram* [1973] 1 All ER 241; *Hubbard* v. *Vosper* [1972] 2 QB 84.

15 *Faccenda Chicken Ltd* v. *Fowler* [1986] 1 All ER 617, cited with favour in cases in Australia, Canada and New Zealand.

from public sources both during and after their employment. It also recognized that the employee's general skill and knowledge is free for an employee to keep and use and cannot be the subject of a breach of confidence claim.

9.34 More controversially, but fairly consistent with US law as expressed in the UTSA, the court in *Faccenda Chicken* recognized a distinction between business information that is merely confidential and business information that constitutes trade secret information. It held that mere confidential information (not amounting to trade secrets) of which the employee has been made aware (either explicitly or implicitly) must be kept confidential and cannot be disclosed during the term of employment. However, at the end of employment such information may be used by the employee unless the employee signed an enforceable non-disclosure agreement to protect that information. In contrast, even in the absence of an express non-disclosure agreement, information deserving of the highest level of protection in the workplace (trade secrets) cannot be used by employees after employment for anyone's benefit other than the employer's.

9.35 As a practical matter, to apply the foregoing distinction requires the subject employees to be aware of the different classifications of information and the duties of confidentiality that apply to each. When it is unclear whether information was provided to an employee in confidence, the *Faccenda* decision provides a set of factors that a court may consider for guidance. These factors are whether: (1) the information is confidential if looked at in isolation; (2) the non-confidential information is clearly severable from the rest of the information; (3) the information could reasonably be regarded as clearly secret or sensitive; (4) the information was necessarily acquired by the employees in order that they do their work; (5) the information was generally known among employees at a junior level or was restricted to senior management; and (6) the employer had given express instructions that the information was to be treated as confidential.[16] All of these factors are consistent with the notice function of the reasonable efforts requirement of US law, as discussed in Chapter 3.

9.36 Where restrictive covenants are entered into with employees, UK courts will evaluate them for reasonableness, particularly if they involve post-employment restrictions. As in the United States, non-compete agreements in the United Kingdom are generally more suspect than non-solicitation agreements and confidentiality agreements and are generally disfavoured. In fact, in the employment context they are considered void unless the employer can establish that they are needed to protect a legitimate business interest and are reasonable in

16 *Ibid.*

terms of what is actually needed to protect that interest.[17] Outside the employment context, restrictive covenants will be evaluated under principles of competition law to determine if they unduly restrict trade or are otherwise anticompetitive.

9.37 Generally, due to the strong public policy against restrictions on free competition, an employer's interest in preventing competition is not a legitimate business interest that will support a non-compete agreement in the United Kingdom (or most other countries), but an interest in preventing the wrongful disclosure or use of trade secrets may be considered a legitimate business interest.[18] The analysis of legitimacy depends upon the nature of the trade secrets, the importance of them to the employer's business and their remaining useful life, among other factors.

9.38 If a legitimate business interest to support a non-compete agreement is found, the agreement will be scrutinized further to determine if it is reasonable in terms of the specific restrictions it imposes on the former employee, the geographic scope of the restrictions and the length of the restrictions. As a practical matter, this means that non-compete provisions that are not tailored to a specific employee and set of information are unlikely to be deemed reasonable. Also, if the trade secrets can be protected effectively through other means, such as a confidentiality agreement or non-solicitation agreement, enforcement of the non-compete agreement may be deemed improper. Judging from reactions of surprise to a recent case of the UK Supreme Court that found a 12-month restriction reasonable,[19] ordinarily the length of acceptable non-compete agreements in the UK will be less than a year.

9.39 There is no requirement in the United Kingdom that an employee who agrees to a post-employment non-compete agreement be paid during the period of non-competition. Also, there is no requirement that the employee be given extra compensation for agreeing to the non-compete agreement. However, as with all contracts, a non-compete agreement in the United Kingdom must be supported by consideration which often is in the form of new or continued employment.

9.40 Because there is no trade secret law, per se, in the UK and confidential information has not been considered to be a form of property, there is not much case law on the issue of ownership of employee-created trade secrets or

17 *Herbert Morris Ltd* v. *Saxelby* [1916] 1 AC 68.

18 *Ibid.*

19 *Vestergaard Frandsen A/S and others* v. *Bestnet Europe Ltd and others* [2013] UKSC 31.

confidential information. However, there is law governing employee-created inventions that should cover most technical trade secrets. Specifically, the UK Patents Act 1977 contains provisions which apply to employee-created inventions. The general rule is that an employer owns all inventions made by an employee within the course and scope of his employment.[20] Similar ownership rules apply to copyrighted works (which may apply to some non-technical employee-created information) pursuant to section 11(2) of the UK Copyrights, Designs and Patent Act 1988.[21] Under some specified circumstances, an employee-inventor may be entitled to compensation from the employer if the invention turns out to be of 'outstanding benefit to the employer'.[22]

D. Trade secrets in business relationships

9.41 Relationships between businesses in the United Kingdom are important in trade secret cases for the same reasons they are important in the United States. The voluntary sharing of trade secret information waives the secrecy of the information unless it is done under the cloak of a confidential relationship. Unlike in the case of the employer/employee relationship, however, a duty of confidence between businesses in the UK will not be readily implied but must be established either by an express agreement or by the circumstances.[23] As detailed above, the common law of breach of confidence in England and Wales defines the circumstances where a confidential relationship may be implied, but no business should rely on an implied duty. Instead, as detailed in Chapter 5, they should acquire a written agreement of confidentiality before sharing any confidential information.

9.42 Businesses in the United Kingdom are generally free to contract about most matters, but agreements in restraint of trade will be scrutinized by competition authorities and may not be enforced by the courts.[24] As a general rule, particularly because agreements between businesses are a matter of competition policy governing restraints on trade and anticompetitive behaviour rather than employment law, as discussed above, non-compete agreements between businesses are more likely to be upheld than non-compete agreements between employers and employees, particularly if they are entered into in conjunction with the sale of a business. Nonetheless, as previously discussed, they may still be evaluated to determine if they are in furtherance of a legitimate business

20 UK Patents Act 1977, s. 39(1)(a).
21 UK Copyrights, Designs and Patent Act 1988, s. 11(2).
22 UK Patents Act 1977, s. 40(2)(b).
23 See e.g., *Seagar* v. *Copydex Ltd* [1967] 1 WLR 923.
24 Bloomberg BNA, *Restrictive Covenants and Trade Secrets in Employment Law: An International Survey* (2011), 'United Kingdom', para. 24.I.B.

interest and are reasonable in terms of scope and duration. For similar reasons, and because they are less restrictive, confidentiality agreements and non-solicitation agreements between businesses are regularly enforced in UK countries as long as they are reasonable.

9.43 As in the United States before the widespread adoption of the UTSA, an issue has arisen in the UK with respect to the liability of third parties for breach of confidence; in other words, where an individual or company derives confidential information, not from the information owner directly, but from another person or company that owed a duty of confidence to the information owner (such as a business to which trade secrets have been licensed). As noted in Chapter 3, the UTSA solved this problem by including a broad definition of misappropriation that imposes liability on third parties provided they had sufficient knowledge of the confidential information and the duty of confidence.

9.44 By common law, UK courts have developed a rule of third party liability whereby knowledge by a third party of the need for confidence may provide the basis for a breach of confidence action against that person, provided that the subject information is not in the public domain at the time the third party acquires the information.[25] However, in keeping with the equitable nature of breach of confidence claims, the rule may not apply to *bona fide* purchasers for value; in other words, those who change position before acquiring, disclosing or using the requisite knowledge.[26] Moreover, what constitutes the requisite knowledge is not well defined in the case law and is subject to equitable considerations that are unpredictable.

E. Criminal consequences for trade secret misappropriation

9.45 As previously noted, the laws and procedures of the four countries that comprise the United Kingdom are not always identical. This is particularly true with respect to criminal laws. Thus, the focus of the following discussion is on the criminal laws of England and Wales which, in contrast to Scottish law, are largely a matter of written code rather than common law.

9.46 Trade secret misappropriation is not currently a crime in England and Wales, and because confidential information is not considered a form of property, its

25 *Attorney-General* v. *Guardian (No. 2)* [1990] AC 109, 260; *Creation Records Ltd* v. *News Group Newspapers Ltd* [1997] EMLR 444.

26 Kate Brearley and Selwyn Bloch, *Employment Covenants and Confidential Information* (3rd edn 2009), para. 6.75.

misappropriation does not fall under the language of the Theft Act either.[27] However, the various 'bad acts' that often accompany the alleged wrongful acquisition of trade secrets may constitute crimes in the UK. For instance, hacking into a computer to acquire trade secret information may constitute a violation of the UK Computer Misuse Act 1990.[28] Under Scottish law, Scots common law might find trade secret misappropriation to be a crime in some situations.

F. Litigating trade secret disputes

9.47 The rules of civil procedure of the courts of each country in the United Kingdom ultimately define how the litigation of trade secret actions will proceed, but generally it begins with the filing of a prescribed claim (known in England as a Statement of the Case).[29] As noted previously, which court a claim is filed in depends upon the monetary value of the claim. Higher value cases in England and Wales are heard by the High Court in London which consists of three divisions: the Chancery Court, the Queen's Bench and Family Courts. Generally, the Chancery Court considers business matters, including patent, copyright and trademarks claims, but actions for breach of confidence are usually assigned to the Queen's Bench division because the offence is considered a tort.[30]

9.48 Once a claim is initiated, it is usually served on the defendant who must acknowledge service. The defendant then has a deadline within which to respond to the claim. Once the defendant files a defence, the court takes over active management and scheduling of the case. Interim (or preliminary) injunctions (known as interdicts in Scotland) may be sought and granted, provided that a sufficient factual and equitable showing is made of the need for such relief.[31]

9.49 Pursuant to the applicable procedural rules of each country within the United Kingdom, pretrial discovery is allowed but is less extensive than the discovery that is allowed in US court proceedings because it is generally limited to the disclosure of documents. For instance, the Civil Procedure Rules (CPR)

27 Grania Langdon-Down, 'Stealing Secrets Goes with the Job', *Independent*, 19 March 1997, available at www.independent.co.uk/news/uk/stealing-the-secrets-goes-with-the-job-1273811.html.

28 *R* v. *Martin* [2013] EWCA Crim 1420.

29 Civil Procedure Rules 2014, Part 16 and accompanying Practice Directions.

30 See *A Guide to the Working Practices of the Queen's Bench Division within the Royal Courts of Justice* (May 2014), para. 1.5.4, available at www.justice.gov.uk/downloads/courts/queens-bench/queen-bench-guide.pdf, describing the work of the Queen's Bench to include tortious conduct and breach of contract claims.

31 Civil Procedure Rules 2014, Rule 25. See also *American Cyanamid* v. *Ethicon* [1985] AC 396.

applicable in England and Wales, Part 31, sets forth the process for the disclosure of documents and generally requires the parties to produce documents on which they rely and which adversely affect their case. CPR Rule 31.17 additionally allows documents to be obtained from third parties under specified conditions. Part 34 concerns summoning witnesses for trial and includes a provision whereby a party can request an order to be able to depose a witness before trial.

9.50 The general rule in the United Kingdom is that court proceedings will be open to the public. However, pursuant to CPR Rule 39.2, in England and Wales a party may request a private hearing for the purpose of protecting confidential information. CPR Rule 5.4 governs the extent to which court records are available to the public. Rule 5.4C(4) provides that a party to a lawsuit may request an order to limit access to court records. Under CPR Rule 25.1, English courts have discretion to grant a long list of interim measures (preliminary relief), but the list does not specifically include the ability to issue a protective order or what is referred to in the UK as a 'non-disclosure injunction'. However, the case management provisions of the CPR give courts the power to 'take any other step or make any other order for the purpose of managing the case and furthering the overriding objective'.[32] Thus, the issuance of non-disclosure injunctions will be granted upon a proper showing.

9.51 The potential remedies for breach of confidence actions in the United Kingdom depend upon how the action is framed; that is, whether it is brought as a breach of contract action, a tort claim based upon an alleged breach of confidence, a property claim or an equitable claim (or all of the above). Generally, however, both permanent injunctive relief and damages are available upon the proper showing. As a practical matter, the availability of damage relief depends upon whether actual harm can be proven, which logically depends upon the extent of the use or disclosure of the subject information. Injunctive relief will not be granted automatically upon a finding of breach of confidence, but will only be granted if warranted. In this regard, consideration will be given to whether the subject information maintains its confidential status and whether there are adequate remedies at law.

9.52 An issue that arises in the UK with respect to injunctive relief is the permissible length of permanent injunctive relief, particularly in light of what is referred to as 'the springboard doctrine'. The general idea behind this doctrine is that a person who breaches a duty of confidence should not be able to benefit from the advantage he gets over other would-be competitors by using information that

32 Civil Procedure Rules 2014, Rule 3.1(m).

he gained in confidence to springboard or jump start a business.[33] This is similar to the 'head-start' concept of US trade secret law discussed in Chapter 3.

9.53 To the extent lengthy or unlimited injunctions are issued by UK courts, the same concerns about the unfairness of such injunctions arise that were addressed by the drafters of the USTA when they expressly limited the permissible length of injunctive relief under US law. However, in the absence of legislation to address this same concern under UK law, any limits on the length of injunctive relief must be recognized at common law. There are cases in the United Kingdom where such limits have been applied, it being recognized that injunctive relief should be limited to the period of advantage.[34]

9.54 An interesting aspect of English law is a procedural device that may be used by trade secret owners to seize information and evidence early in the life-cycle of a breach of confidence case. Known as an 'Anton Piller order' based upon an early case that recognized the remedy[35] (and also known as a civil seizure order), this remedy has subsequently been recognized in other common law jurisdictions including Canada,[36] India, New Zealand, Singapore[37] and Hong Kong, among others. However, based upon principles that have developed in England since the initial recognition of the remedy, it should only be granted in exceptional cases.

9.55 The facts of *Anton Piller* are illustrative of the narrow circumstances in which this extraordinary order was originally meant to apply. Anton Piller KG, a German producer of computer components, was getting ready to release a new product. However, its English agent, a company called Manufacturing Processes Ltd (MPL), was secretly colluding with German competitors as well as firms in Canada and the United States to appropriate Anton Piller's designs. When Anton Piller learned of the scheme it decided to bring suit, but feared that once the defendants were served notice of the suit they would destroy the information or send it to Germany, beyond the jurisdiction of the British court.

9.56 Anton Piller's solicitor sought an *ex parte* interim injunction and order directing MPL to consent to an inspection of its premises in order to search for the documents in question. When the court of the first instance declined to grant

33 *Terrapin* v. *Builders Supply* [1967] RPC 375.

34 See e.g., *EPI Environmental Technologies, Inc.* v. *Symphony Plastic Technologies* [2006] EWCA Civ 3, available at www.bailii.org/ew/cases/EWCA/Civ/2006/3.html.

35 *Anton Piller KG* v. *Manufacturing Processes Ltd and others* [1976] 1 Ch. 55. See also *EMI Ltd* v. *Pandit* [1975] 1 WLR 302.

36 Bloomberg BNA, *Restrictive Covenants and Trade Secrets in Employment Law: An International Survey* (2011), 'Canada'.

37 Gladys Mirandah and Gerald Samuel, *Trade Secrets Throughout the World* (2013), vol. 3, para. 33:23.

the inspection order, the matter was appealed and the appellate court reversed and granted the inspection order. The appellate court was careful to specify that such an order should be granted only in exceptional circumstance and that the order was not a civil search warrant. Instead, it was an order requiring the defendant, on penalty of being held in contempt, to consent to the search.

9.57 The appellate court specified three conditions which must be met before an Anton Piller order will be granted: (1) the plaintiff must have an 'extremely strong' *prima facie* case; (2) the damage, potential or actual, must be 'very serious'; and (3) the plaintiff must present clear evidence that the defendant possesses incriminating documents or other items and show that there is a 'real possibility' that the defendant may destroy such items once informed of the plaintiff's application. The court also imposed some procedural safeguards to prevent abuse of the order. First, the court directed that the plaintiffs carry out their search in the presence of their solicitor, an officer of the court. Second, the defendants must be given an opportunity to consider the order and consult their own solicitor. If the defendant refused to comply, the plaintiffs were not to force their way in, but accept the defendant's decision; the parties could then return to court to argue the issue.

9.58 In 1999, the Anton Piller order (and its limitations) was codified into Rule 25.1(1) of the CPR (applicable in England and Wales) and is now properly known as a 'search order'. A motion for a search order can be sought at any time, be it before litigation or afterwards to enforce a judgment. However, only a judge may grant such an order, and generally, county courts are prohibited from issuing them.[38]

9.59 Pursuant to the CPR, an applicant for a search order must establish the following four elements:

(1) that there is a strong *prima facie* case that the defendant has committed the acts alleged in the complaint;
(2) that the defendant's actions have caused very severe actual or potential damage to the claimant;
(3) that there is a real and serious possibility that the defendant will destroy documents or other evidence in its possession; and
(4) that a search order is not excessive and out of proportion.[39]

---

38 Bloomberg BNA, *International Patent Litigation: A Country-by-Country Analysis* (2011), 'United Kingdom (GB)', para. IX.10.c. See also County Court Remedies Regulations 2014 (SI 2014/982).

39 Hilary Pearson, *Trade Secrets Throughout the World* (2013), vol. 3, 'United Kingdom', para. 39:34.

If granted, the order is subject to numerous safeguards required by CPR Rule 25. Among other requirements: (1) a 'supervising solicitor' must be present and cannot be from the same firm as the applicant's own solicitor; (2) the search must be carried out during normal business hours; and (3) the supervising solicitor must inform the respondent of their legal rights.[40]

9.60 Anton Piller orders are not recognized in Scotland, but similar relief may be available based upon other theories and procedural devices, for instance, as part of an order for preliminary relief.

III. CANADA

A. Overview of the legal system

9.61 Like the United States (and many other countries), Canada was inhabited by aboriginal peoples long before the first European settlers arrived in the fifteenth century, but much of its history since then was influenced by those European settlers. For present day purposes, the most important influences were the result of the presence of both French and British settlers, including the French fur traders of the early 1600s. While the British started arriving in Canada as early as 1583, the influence of Britain on the history and legal traditions of Canada was solidified following the Seven Years' War and the signing of the Treaty of Paris in 1763 whereby France ceded most of its North American territory to Britain.

9.62 Essentially, the Canada of today began as a combination of four provinces and grew over time as more provinces and territories were added. The recognition of Canada as an autonomous and sovereign nation also occurred over time, first with the Statute of Westminster 1931 and later with the Canada Act 1982, both Acts of the British [UK] Parliament.

9.63 Owing to its history as a battleground between the French and British, Canada has two official languages (English and French) and follows both the common law and civil law legal traditions. The richness of Canada's bilingualism is reflected in its population, approximately 75 per cent of whom speak English and the remaining 25 per cent speak French. The Canadian Parliament is required under the Constitution to use both English and French in its proceedings and its publications, and it enacts legislation in both languages.

40 *Ibid.*, quoting CPR Practice Direction 25A, 25APD.7.

9.64 Canada's dual legal system is officially part of the British North America Act 1867 which established four British colonies as a confederation called the 'Dominion of Canada'. It was later recognized and confirmed in the Canada Act 1982. Similar to the US system, it allows for both national and provincial (or territorial) legislatures to enact laws, subject to some instances of exclusive jurisdiction. For instance, it allows for exclusive provincial jurisdiction with respect to property rights and civil rights and exclusive federal jurisdiction with respect to various matters of national concern. Accordingly, the province of Québec has created its own Civil Code (Civil Code of Québec) to govern its private law. However, while the Civil Code governs private law in Québec, Québec is subject to the same public law as the rest of Canada. This includes constitutional and criminal laws. Moreover, the civil and common law systems in Canada are becoming quite similar to each other, as the civil law recognizes more case precedent and the common law jurisdictions continue to adopt more legislation.

9.65 The Canadian federation consists of nine provinces that are based on the common law tradition, three territories that are also based on the common law tradition, and one civil law province, Québec. Canada has a federal Parliament (based in Ottawa) which legislates for all of Canada with respect to matters of national concern. In addition each province and territory has its own legislature to deal with local matters.

9.66 The national government of Canada consists of three branches of government: the executive branch, the legislative branch and the judiciary. The executive branch includes the Monarch (currently Queen Elizabeth II, but represented in Canada by the Governor General), the Prime Minister and the Cabinet. This branch implements the laws while the legislative branch makes the laws. The legislative branch (the Parliament) consists of the House of Commons, the Senate and the Monarch. The members of the Senate are appointed by the Governor General, while membership in the House of Commons is by democratic election. Thus, Canada is a constitutional monarchy with a parliamentary democracy that recognizes the Queen or King as the Head of State and the Prime Minister as the head of government.

9.67 The judicial branch of Canada is comprised of courts at both the federal and provincial (or territorial) levels. The federal court system in Canada consists of Federal Tribunals, the Federal Court of Canada and the Supreme Court of Canada. The federal courts handle matters that are outside the territorial jurisdiction of any province or territory and certain specialized areas of federal law. Similar to the federal court system in the United States, the route for an appeal is from the trial division of a federal court to the Federal Court of Appeal

and then on to the Supreme Court. The Supreme Court of Canada is the highest court. It hears disputes arising both from civil and common law jurisdictions. Québec has guaranteed representation on the Supreme Court of Canada (three of the nine judges must be chosen from Québec). In addition to the federal court system, the provinces each have superior, county and district courts. The names and jurisdictions of some of these courts may vary, but they also have both trial and appellate divisions.

9.68 Except for the courts of Québec, the courts of Canada follow the common law tradition and develop much of the applicable law through case decisions. When a court in Canada has not previously ruled on an issue, it will consider the decisions of other common law courts within Canada. Furthermore, it is not uncommon for such courts to consider decisions by the courts of England. While decisions from American courts may also be considered, they do not generally have the same persuasive effect that decisions of English courts enjoy.

9.69 Canada is a long-time member of both the Berne Convention and the Paris Convention, having acceded to those agreements on 10 April 1928 and 21 August 1923, respectively. It is also an original member of the WTO Agreement, effective 1 January 1995, and a member of GATT since 1 January 1948. Canada is also a party to the North American Free Trade Agreement (NAFTA) (along with the United States and Mexico). Consistent with Article 39 of the TRIPS Agreement, NAFTA requires a minimum standard of protection of trade secrets.[41] For more on the relevance of these agreements, see the discussion in Chapter 2 and the discussion of NAFTA in the section on Mexico, below.

B. Contours of trade secret protection

9.70 Similar to the United States, the Canadian national government grants patents, trademarks and copyrights, but there is no federal trade secret law except that, as is discussed below, there can be a criminal misappropriation of trade secrets under the federal law of Canada. As in the United States, the law of trade secrets in Canada is principally based upon the laws of each province and territory of Canada and, accordingly, can differ except with respect to issues that have been ruled on by the Supreme Court of Canada. Accordingly, the discussion that follows provides general principles that tend to govern in most of the provinces and territories. The specific laws and case decisions of each province and territory should be researched to determine any nuances in the application of the general principles.

41 See Chapter 2.

9.71 As noted earlier, Canada is primarily a common law country and accordingly (except in Québec) its trade secret principles have developed as part of the tort of breach of confidence through the common law process. To date, Canada has not codified its trade secret law and, with the exception of the enacted laws of Québec discussed below, none of its provinces or territories have enacted trade secret legislation. Generally, the trade secret law of Canada is similar in scope and application to the trade secret law of England and Wales (as described above) and borrows heavily from it, but it also includes many aspects of US law.[42]

9.72 In 1989 the Uniform Law Conference of Canada adopted a Uniform Trade Secrets Act and recommended that the common law provinces adopt it, but as of the date of publication of this book, it has not been adopted by any of the individual provinces or territories.[43] Nonetheless, it does provide some guidance regarding Canadian law, in effect serving as a restatement of the common law of trade secrets in Canada.

9.73 As in England and Wales, Canada's common law of breach of confidence applies to trade secret claims by protecting qualifying confidential information from wrongful use or disclosure. There are a number of definitions of confidential information under Canadian case decisions. In a leading case, the court borrowed heavily from the US definition of a trade secret and, in fact, quoted from several US case decisions, all of which predate the adoption of the UTSA.[44] The terms 'trade secrets' and 'confidential information' appear to be used interchangeably in Canada. In contrast, Québec cases often use the term 'trade secrets' to refer to technical trade secrets and 'confidential information' to refer to business information.

9.74 As case law has developed in Canada, the common elements underlying that which is deemed 'confidential information' are that the information: (1) is used in business; (2) is not generally known; (3) derives its value from being unknown; and (4) must be subject to reasonable efforts to keep it secret.[45] Virtually any kind of information used in business can be a trade secret. However, information that is part of the public knowledge or public domain

---

42 See generally, K.G. Fairburn and J.A. Thorburn, *Law of Confidential Business Information* (2007).

43 See Uniform Trade Secrets Act, Uniform Law Conference of Canada 1989 (Can.), available at www.ulcc.ca/en/2011-winnipeg-mb/537-josetta-1-en-gb/uniform-actsa/trade-secrets-act/730-uniform-trade-secrets-act-1989.

44 *R.L. Crain Ltd* v. *Ashton Press Manufacturing Co. Ltd* [1949] OR 303 (Can.).

45 See e.g., *Software Solutions Associates Inc.* v. *Depow* (1989) 25 CPR (3d) 129, 138–9 (Can. NBQB); *Belform Insulation Ltd* v. *Toleks Insulation Ltd* (1998) 85 CPR (3d) 160, 163 (Can. Ont. Gen. Div.); *Techform Products Ltd* v. *Wolda* (2000) 5 CPR (4th) 25, 50 (Can.).

cannot be the subject of a breach of confidence claim.[46] Also, although confidential information as a whole may contain some parts that are publicly known, the overall nature of the information must not be public.

9.75 Even though the terms 'trade secret' and 'confidential information' tend to be used interchangeably in Canada, confidential information appears to include a broader range of information, some of which can be trade secrets.[47] In keeping with the breach of confidence principles of England and Wales, generally confidential information can include personal information, business information and ideas. What sets protectable information apart is that it is not generally known to the public and there is some aspect of novelty to it.

9.76 Canadian courts generally use a six factor test (borrowed from the *Restatement (First) of Torts* in the United States) to determine whether information qualifies as a trade secret. These six factors are: (1) the extent to which the information is known outside the owner's business; (2) the extent to which it is known by employees and others involved in the owner's business; (3) the extent of measures taken by him to guard the secrecy of the information; (4) the value of the information to him and his competitors; (5) the amount of money or effort expended by him in developing the information; and (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.[48]

9.77 Confidential information must be identifiable and the owner must be able to say specifically what it is that is secret.[49] It should not be vague or a matter of general knowledge. If the information is not identifiable then it becomes more difficult to distinguish it from publicly available information or general knowledge. The requirement of identification also makes the rights of the parties more predictable.

9.78 Consistent with US law, ideas can be protected as trade secrets in Canada but they must have some element of novelty or originality. However, information need not be novel in the patent law sense. Rather, the information cannot be of a 'trivial' nature or 'easily accessible from public sources'.[50] Also consistent with US law, while information that is entirely public does not qualify for trade secret protection in Canada, if the information forms a so-called 'combination trade

46 See *Promotivate International Inc.* v. *Toronto Star Newspapers Ltd* (1985) 23 DLR (4th) 196, 53 OR (2d) 9 (Can. HCJ).

47 See Ronald E. Dimock, *Intellectual Property Disputes: Resolution and Remedies* (2002), para. 5.3.

48 *Pharand Ski Corp.* v. *Alberta*, 1991 Carswell Alta. 85, 37 CPR (3d) 288, 316; 80 Alta. LR (2d) 216 (Can. QB).

49 See *Cadbury Schweppes Inc.* v. *FBI Foods Ltd* [1999] 1 SCR 142, 235 NR 30 (Can.).

50 *Faccenda Chicken Ltd* v. *Fowler* [1986] 1 All ER 617, 731 (UK).

secret' such that some of it is in the public domain while the rest of it is not, it may nonetheless be eligible for protection. However, the confidential parts of the combination must have enhanced the overall value of the combination, including that which was in the public domain.[51]

9.79 Canadian law requires that some efforts be taken to maintain secrecy of information in order for it to be protected by trade secret law. Absolute secrecy of the information is not required. Rather, as in the United States, the standard is one of relative secrecy. Canadian law also requires that the information be of some value. One court divided confidential information into three categories to signify its value: 'nothing very special', 'something special' and 'very special indeed'.[52] The information has to be more than 'nothing very special' to be protectable under Canadian law.

9.80 Similar to the historic origins of trade secret law in England and the United States, the law of confidential information in Canada is meant to promote standards of commercial morality and prevent the misappropriation of confidential information, including trade secrets. Generally, to establish misappropriation, a breach of confidence must be shown. However, Canadian law also recognizes an action for misappropriation based upon a claim of breach of confidence by improper means.[53]

9.81 No contractual relationship is required to create a duty of confidence in Canada. Rather, similar to English and US law concerning the establishment of implied at law duties of confidentiality, if a defendant has used a trade secret he obtained from a plaintiff without consent, he is guilty of misappropriation of the trade secret.[54] The law appears to be based on equitable principles that protect information that was delivered in confidence from being used for unfair advantage by the recipient of the information.[55] Generally, this duty to maintain confidentiality remains as long as the information continues to be kept secret by the owner.[56] However, even when information that was disclosed under terms of confidence enters the public domain, the recipient may still have a duty to maintain confidentiality co-extensive with any head-start (or lead-time) he may have obtained while being privy to the information.[57]

---

51 *International Corona Resources Ltd* v. *LAC Minerals Ltd* [1989] 2 SCR 574, 1989 Carswell Ont. 965, 44 BLR 1, 78 (Can.).

52 *Cadbury Schweppes Inc.* v. *FBI Foods Ltd* [1999] 5 WWR 751, para. 65 (Can.).

53 *Pharand Ski Corp.*, 80 Alta LR (2d), n. 48 above, at 239.

54 *Ibid.* 239, quoting Lord Greene in *Saltman Engineering Co. Ltd* v. *Campbell Engineering Co. Ltd* (1948) 65 RPC 203, [1963] 3 All ER 413n (UK CA).

55 John T. Ramsay and Francois Grenier, *Trade Secrets Throughout the World: Canada* (2013), para. 6:13.

56 *Ibid.* para. 6:17.

57 *Cadbury Schweppes Inc.*, [1999] 5 WWR 751, n. 52 above, at para. 67.

9.82 To establish a breach of confidence in Canada, the plaintiff must prove that: (1) the information was confidential; and (2) that the information was imparted under circumstances suggesting an obligation of confidence. Information that is communicated in a public manner will negate any duty of confidentiality. Misappropriation may also be established by proving that there was an unauthorized use of the information to the detriment of the plaintiff.[58] In a departure from the majority view under US law, if a former employee misappropriates confidential information belonging to his former employer, his new employer may be vicariously liable for his misconduct.[59]

9.83 Trade secret protection in Canada does not forbid reverse engineering and independent development. Also, similar to the law in California which places the burden on the defendant to prove that information was readily ascertainable, selling a product that is capable of being reverse engineered does not necessarily mean that trade secret protection in the product has been lost as a result of it being offered for sale or available publicly.[60] It depends on whether the information disclosed in the product is readily ascertainable.

9.84 The Civil Code of Québec regulates trade secret law in that province.[61] Various sections of the Civil Code relating to civil and contractual duties are those applicable in trade secret cases. For instance, one section provides generally that a person should 'abide by the rules of conduct which lie upon him according to the circumstances, usage or law so as not to cause injury to another'.[62] Another provides that 'every person has a duty to honour his contractual undertakings'.[63] No significant differences appear to exist in the basic principles applied in Québec compared to the other Canadian provinces and territories due to the fact that equitable and common law principles are often integrated into the civil law of Québec. Accordingly, while the Civil Code itself does not specifically deal with trade secrets, the governing law tends to be interpreted from the judge-made common law.

C. Trade secrets in employment relationships

9.85 Several general principles of Canadian jurisprudence apply to confidentiality in employer-employee relationships. Generally, employees owe a duty of good

58 *International Corona Resources Ltd*, [1989] 2 SCR 574, n. 51 above.

59 See *Apotex Fermentation* v. *Novopharm* (1995) 63 CPR (3d) 77 (Can. Man. QB).

60 See Barry Sookman, *Computer Law: Acquiring and Protecting Information Technology* (1997).

61 The relevant provisions relating to trade secrets or confidential information can be found in arts 1310, 1434, 1457, 1601 and 1602 of the Civil Code of Quebec, SQ 1991, c. 64 (Can.).

62 *Ibid.* art. 1457.

63 *Ibid.* art. 1458.

faith and loyalty to their employers and they may not act to the detriment of the employer during the course of employment. At a minimum, an employee must maintain the confidentiality of the employer's trade secret and confidential information, including customer lists.[64] Also, absent a contract, some obligations may be implied both during and after termination of employment.

9.86 Employers in Canada may choose to increase the level of their employee's obligations via contract. Senior or top management employees may also be held to a higher standard and be subject to higher duties as directors of the company.[65] For instance, these high-level employees or officers may have fiduciary duties to the company. However, if an employee has entered into a valid contract which imposes a duty of confidentiality on use of the employer's information, the courts will be reluctant to imply additional obligations not contained within the document.[66]

9.87 After termination of employment the employee's duties in terms of confidentiality may be more limited depending on the nature of the information, whether it qualifies as a trade secret and whether the employee had significant access to trade secrets during the employment. As one court held, even without an express contract a former employee who acquired knowledge of trade secrets during the course of his employment remains under an implied obligation not to use that information even upon leaving the employer.[67]

9.88 The English case of *Faccenda Chicken* v. *Fowler*,[68] discussed above, has been applied in Canada to limit the categories of information in respect of which an employee may be subject to a duty of confidentiality. Thus, confidential information in the employment setting does not include publicly available information and an employee's general skill and knowledge. However, information receiving the highest level of protection in the workplace, trade secrets, cannot be used by the employee for anyone's benefit other than the trade secret owner's. When it is unclear whether information was provided to an employee in confidence, the *Faccenda* decision also provides a set of factors that a court may consider for guidance (discussed above in the UK section).

9.89 As more fully discussed in Chapter 4, but consistent with Canadian law, it is recommended that an employer wishing to protect confidential and trade secret information enter into an express confidentiality agreement with employees or

64 *Canadian Aero Service Ltd* v. *O'Malley* [1974] SCR 592, 40 DLR (3d) 371, 381 (Can.).
65 *Ibid.* 381.
66 *Faccenda Chicken Ltd*, [1986] 1 All ER, n. 50 above, at 625–6.
67 *R.L. Crain Ltd*, 11 CPR 143, n. 44 above, at 149.
68 *Faccenda Chicken Ltd*, n. 50 above.

others who will be given access to the information. These agreements (also referred to as non-disclosure agreements) aim to protect confidential information by setting out specific obligations on the part of the party receiving the information and are generally enforceable in Canada. However, when drafting a confidentiality agreement, special care should be taken to identify and define the kinds of information that will be considered confidential. On the other hand, the recipient of a confidentiality agreement should be mindful of very broad definitions and might want to limit the scope or otherwise assert certain exclusions so as not to later be held liable for a breach.

9.90 Under Canadian law, a former employee may establish a business in competition with his prior employer and is entitled to use the general skill and knowledge that he gained during that employment in doing so.[69] He may not solicit customers whose information was maintained in confidence by the employer, but he may be permitted to solicit customers based upon information that is publicly available. As previously discussed, information regarding an employer's customers will be deemed confidential when it was known to the former employee by virtue of his or her employment.[70]

9.91 Consistent with the law of most US states, non-compete agreements are enforceable in Canada if they are for the purpose of protecting a legitimate business interest and are reasonable and limited in time and geographic scope.[71] Employment contracts that restrain an employee receive closer scrutiny in general than those contracts accompanying the sale of a business. The more narrow a restriction in terms of time and scope, the more likely it is to be enforced. This is because it is assumed to impose less of a burden on the employee. Also, restrictions are more likely to be enforced against key employees who had greater access to confidential information. Such restrictive covenants are justified to protect the proprietary interests of the business but may not be used solely to prevent competition. Thus, an employee may be restrained only when necessary to protect an employer's proprietary rights.

9.92 The burden of establishing that a covenant is reasonable falls upon the party to whose benefit it inures. In considering whether an employee should be restrained, the effect on competition or on preventing the employee from using his general skill and knowledge will be weighed heavily by Canadian courts. If a restrictive covenant contained in an employment contract is found to be unenforceable, it does not render the entire contract void, since the court may

69 *R.L. Crain Ltd*, 11 CPR 143, n. 44 above, at 149.

70 *Franklin Supply Co.* v. *Midco Supply Co.* (1995) Carswell Alta 308 (Can. Alta. QB).

71 Civil Code of Quebec, SQ 1991, c. 64, art. 2089 (Can.).

sever that part of the agreement and enforce the remaining provisions. Agreements between employers not to employ each other's former employees are void as a matter of public policy.

D. Trade secrets in business relationships

9.93 Canada has a sophisticated and well-developed body of commercial and contract law to govern business-to-business relationships and generally follows principles of freedom of contract. Thus, businesses are usually free to contract among themselves with respect to the licensing and use of trade secrets and other confidential information. As noted above with respect to employee relationships, non-disclosure agreements will generally be enforced in Canada as long as they are reasonable.

9.94 Similar to the idea submission law of the United States, breaches of confidence can occur in Canada in relation to precontractual negotiations between parties if confidential information was disclosed in the process of trying to put together a deal. Claims for breach of confidence may also occur if an inventor who is seeking funding from a company claims that the company later used the information without permission. One court has held that 'where information of commercial or industrial value is given on a business-like basis with some avowed common object in mind, such as a joint venture or the manufacturer of articles by one party for the other, I would regard the recipient as carrying a heavy burden if he seeks to repel a contention that he was bound by an obligation of confidence'.[72] In other words, an implied obligation of confidence is likely to be found on those facts.

9.95 Based upon the foregoing, companies doing business in Canada (as elsewhere) should exercise special care when receiving unsolicited materials from businesses or individuals. This is especially so if they consider the information confidential. Since Canadian common law courts do not require an express understanding when information is disclosed in confidence, it is possible that one may later argue that its information (even if unsolicited) was conveyed in confidence. Accordingly, as further discussed in Chapter 4, the safer practice may be not to receive such information without an express waiver of confidentiality or to return it unopened to the sender.

---

72 *Tree Savers International Ltd* v. *Savoy* [1992] 2 WWR 470, 87 DLR (4th) 202, 205 (Can. CA), quoting *Coco*, [1969] RPC, n. 5 above, at 48.

9.96 With respect to third parties, if a person has actual knowledge that he or she is receiving information that is the subject of a breach of confidence, the obligation to maintain the confidentiality of the information follows. Any unauthorized use of that information could result in liability for misappropriation.[73] Thus, even third parties having no direct involvement in the original disclosure of a trade secret may be liable for breach of confidence under Canadian law.[74] A third party can have constructive or actual knowledge that information is confidential; actual knowledge is not required.[75]

E. Criminal consequences for trade secret misappropriation

9.97 Unlike in the United States but like the United Kingdom, criminal sanctions for the theft of trade secrets are not available in Canada (except for that provided under the Security of Information Act, discussed below). In part, this is because confidential information is not considered property under the Criminal Code.[76] Additionally, the Criminal Code does not contain provisions addressing trade secrets, per se. Traditional offences of theft, conversion and fraud may provide limited relief with respect to some acts of misappropriation. However, these property-related crimes do not easily fit the taking of the kinds of information that constitute trade secrets.

9.98 The Canadian federal government has enacted the Security of Information Act (SIA) that applies throughout Canada. The SIA makes it a criminal offence to use a trade secret for the benefit of a foreign economic entity. It appears to be similar to section 1831 of the Economic Espionage Act in the United States (discussed in Chapter 6) in that it criminalizes the use of a trade secret for the benefit of a foreign entity.

9.99 The SIA provides in section 19(1) that: 'Every person commits an offence who, at the direction of, for the benefit of or in association with a foreign economic entity, fraudulently and without colour of right and to the detriment of Canada's economic interests, international relations or national defence or national security (a) communicates a trade secret to another person, group or organization; or (b) obtains, retains, alters or destroys a trade secret'. Section 19(4) defines 'trade secret' as 'any information, including a formula, pattern, compilation, program, method, technique, process, negotiation position or strategy or any information contained or embodied in a product, device or

73 *Ibid.*
74 *Cadbury Schweppes Inc.*, [1999] 5 WWR 751, n. 52 above, at para. 19.
75 *Ibid.*
76 *R* v. *Stewart* [1988] 1 SCR 963, para. 33.

mechanism that: (a) is or may be used in a trade or business; (b) is not generally known in that trade or business; (c) has economic value from not being generally known; and (d) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy'.

F. Litigating trade secret disputes

9.100 Civil disputes relating to trade secret law in Canada can only be initiated in provincial or territorial courts. In addition to breach of confidence claims, a plaintiff may seek civil remedies, where appropriate, on such grounds as unlawful interference with contractual relationships, breach of fiduciary duty, fraudulent misrepresentation, unjust enrichment and inducing a breach.[77]

9.101 Consistent with the leading case in the United Kingdom, to establish a claim for breach of confidence in Canada a plaintiff must prove three things.[78] First, that the information was confidential. Information that is part of the public domain cannot be the subject of a breach of confidence claim. Although confidential information as a whole may contain some parts that are publicly known, the overall nature of the information must not be public. Second, the information must have been imparted under circumstances suggesting an obligation of confidence. Information that is communicated in a public manner will negate any duty of confidentiality. Third, it must be established that there was an unauthorized use of the information to the detriment of the plaintiff.

9.102 Courts in Canada have discretion to order that pleadings and other materials that contain trade secrets or confidential information be sealed or kept confidential during litigation.[79] Thus, portions of the trial or other proceedings may be held *in camera*.

9.103 A wide range of remedies is available in breach of confidence cases in Canada and courts have flexibility and discretion in choosing the most appropriate remedy for the circumstances. Injunctions barring the continuing use of confidential information are generally awarded. A plaintiff's loss may also be compensated through damages. Where necessary, an accounting of the defendant's profits may be available. A constructive trust over funds received as a result

77 John T. Ramsey and Francois Grenier, *Trade Secrets Throughout The World: Canada* (2011), para. 6:37.

78 *International Corona Resources Ltd*, n. 51 above.

79 See Courts of Justice Act, RSO 1990, c. 43, s. 137(2) (Can.); Fed. Ct R, Rule 151 (Can.), 1998, SOR/98–106; *Amer-Can Development Corp.* v. *Tele Time Saver Inc.* (1976) 1 CPC 230 (Can. Ont. HC).

of improper use of the confidential information may also be imposed. However, in breach of fiduciary duty cases, only equitable remedies may be available to the plaintiff.[80]

IV. INDIA

A. Overview of the legal system

9.104 Owing, in part, to its former status as a British colony from the mid-nineteenth century until its independence in 1947, India is primarily a common law country. However, although it retains a legal system based on the British common law tradition, and often references and applies UK common law, the supreme law of the land is the post-colonial Constitution of 1949 which defines the country as an independent, secular, socialist democracy.

9.105 The Constitution of India establishes a federal system of government that is similar to the US system in that there are states within India that have their own laws, processes and traditions.[81] The country is divided into 29 states and six union territories administered by the national government. Each state elects its own government and each union territory is led by an administrator appointed by the national government.

9.106 The national law-making body is a bicameral Parliament consisting of an upper house, Rajya Sabha (the Council of States), and a lower house, Lok Sahba (the House of People). A President and a Council of Ministers make up the executive branch. The President is elected by the union and state legislatures and serves a term of five years. However, the President is largely a figurehead and the real power lies with the Council of Ministers. This Council is headed by the Prime Minister, who is chosen by Parliament and usually represents the majority party.

9.107 India's judicial branch consists of district courts, an appellate High Court and a Supreme Court.[82] The Supreme Court has original jurisdiction over matters involving fundamental rights as well as interstate and state-Union matters, as well as appellate jurisdiction over the High Courts. As with the UK and US

80 Ramsay and Grenier, n. 55 above, at para. 6:41.

81 *Ibid*.

82 Vinay Vaish *et al.*, *International Civil Procedure: 1* (2003). See also 'Indian Courts', available at http://indiancourts.nic.in/courts/home1.html#.

systems, the pronouncements of the Supreme Court take precedence over lower appellate court decisions.

9.108 Although the law of India is primarily based upon common law, additional sources of law include: the Constitution; national, state and union laws; and treaty obligations. It also includes a written Code of Civil Procedure that dates from 1908 and a written Penal Code. As a practical matter, the various sources of law make finding the applicable law more difficult since there is not one written code where baseline trade secret principles can be found. However, because English is spoken widely throughout the country, many judicial opinions and secondary sources of law are available in English.

9.109 Compared to other countries, India has not been quick to join international agreements concerning the protection of intellectual property rights (IPRs), having only done so in the twentieth century. In this regard, India is a signatory of the Berne Convention as of 1 April 1928 and the Paris Convention as of 7 December 1998. While India is a founding member of both GATT and the WTO, as a developing country it was not required to comply with the provisions of the TRIPS Agreement until 1 January 2000.[83] Furthermore, treaties are not self-executing in India, requiring India to comply with its international commitments either by enacting specific laws or by developing the required legal principles through the common law process or the interpretation of pre-existing administrative regulations, statutes and constitutional provisions.

B. Contours of trade secret protection

9.110 The United States Trade Representative has placed India on its Special 301 Priority Watch list for every year the list has existed, recently characterizing India's IPR framework as 'weak' and detailing 'serious concerns' in many areas.[84] The reasons for the weakness in India's IPR enforcement are varied and complex, having as much to do with the lack of timely and efficient judicial proceedings and remedies as it has to do with the details of applicable law. This weakness is particularly true with respect to trade secret law because, unlike the laws governing patents, copyrights, trademarks and industrial designs, there is currently no detailed statutory trade secret law in India that is similar to the

83 Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), 15 April 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 'The Legal Texts: The Results of the Uruguay Round of Multilateral Trade Negotiations' (1999), p. 320, Part IV, Arts 65–66, 1869 UNTS 299, (1994) 33 ILM 1197.

84 Office of the US Trade Representative, *2014 Special 301 Report* (2014), available at www.ustr.gov/sites/default/files/USTR%202014%20Special%20301%20Report%20to%20Congress%20FINAL.pdf.

UTSA. Instead, as discussed in more detail below, trade secrets in India must ordinarily be protected by contract or vindicated through an assortment of common law tort doctrines, principally a breach of confidence claim.

9.111 An early member of the WTO and an important developing country, India was an active participant in the NG11 negotiations that led to the TRIPS Agreement. As previously noted in Chapter 2, however, India was one of a number of developing countries that were reticent to classify trade secrets as a form of intellectual property, preferring instead to categorize trade secret misappropriation claims as a form of unfair competition. This position, and the fact that India (and the United Kingdom on which much of its trade secret law is based) already had a developed body of unfair competition law at the time the WTO Agreement was approved, explains why India did not believe it was necessary to adopt a trade secret statute.

9.112 To be fair, but for the fact that India's judicial system is cumbersome and backlogged such that the needs of trade secret plaintiffs' often cannot be addressed in a timely manner, the state of trade secret law in India is similar to the laws that existed in the United States before the widespread adoption of the UTSA. Thus, like the law of the England (before it must comply with an EU Trade Secret Directive) and the law of the United States (before the widespread adoption of the UTSA), the best way to think about the trade secret law of India is as an amalgam of various common law tort, contract, unfair competition and equitable claims for relief, with some statutes thrown into the mix. Superimposed over this collection of claims is the fact that not many case decisions have been rendered in India with respect to trade secret matters and, accordingly, the common law of trade secrecy has not had much chance to develop.

9.113 Despite the absence of a detailed trade secret law similar to the UTSA, Indian courts have recognized the existence and protectability of trade secrets for many years, although the definition of trade secrecy has been described as 'somewhat fluid'.[85] More recently, in light of the ongoing economic boom in India, especially in data sensitive fields such as knowledge process outsourcing, Indian courts have shown increasing willingness to protect trade secrets and, over time, a rough definition of trade secrecy has emerged.

85 Sonia Baldia, 'Offshoring to India: Are Your Trade Secrets and Confidential Information Adequately Protected?' (2010) *Business and Technology Sourcing Review* 9; Sahil Taneja and Samrid Bharwaj, 'The Viability of Trade Secret Protection' in *India: Managing the IP Lifecycle* (IP Media Group, 2013), p. 13.

9.114 Importantly for attorneys who wish to enforce trade secrets in India, Indian courts are willing to consider case decisions from other countries, particularly the United Kingdom and the United States, and thus this non-binding law should be used to help speed the development of trade secret principles in India. For instance, in *Konrad Wiedemann GmbH* v. *Standard Castings Pvt Ltd*,[86] the Indian High Court quoted the English case *Saltman Engineering Co. Ltd* v. *Campbell Engineering Co. Ltd*,[87] defining the elements of trade secrecy as:

> The information to be confidential must, I apprehend, apart from contract, have the necessary quality of confidence about it, namely, it must not be something which is public property and public knowledge. On the other hand, it is perfectly possible to have a confidential document, be it a formula, a plan, a sketch or something of that kind, which is the result of work done by the maker upon materials which may be available for the use of anybody; but what makes it confidential is the fact that the maker of the document has used his brain and thus produced a result which can only be produced by somebody who goes through the same process.

9.115 By 2010, in a case before the High Court of Bombay, the following six-factors were used to determine whether information qualified for trade secret protection:

(1) the extent to which the information is known outside the business;
(2) the extent to which it is known to those inside the business, i.e. by employees;
(3) the precautions taken by the holder of the trade secret to guard the secrecy;
(4) the savings effected and the value to the holder in having the information as against competitors;
(5) the amount of effort or money expended in obtaining and developing the information; and
(6) the amount of time and expense it would take others to acquire and duplicate the information.[88]

This is the same 'six-factor test' that is listed in the *Restatement (First) of Torts* which, as discussed in Chapter 3, was the predominant source of trade secret law in the United States until the late 1980s. Although not stated directly, this list references the secrecy, commercial value and reasonable efforts requirements of trade secret law as set forth in both the UTSA and Article 39.2 of the TRIPS Agreement.

---

86 [1985] (10) IPLR 243.
87 [1948] 65 RPC 203.
88 *Bombay Dyeing and Manufacturing Co. Ltd* v. *Mehar Karan Singh*, 2010 (112) Bom. LR 375.

9.116 As in other jurisdictions, Indian courts have been reluctant to establish a rigid formula or exhaustive list of subject matter eligible for trade secret status, and theoretically, any sort of information meeting the foregoing criteria could meet the definition of a trade secret. However, because the law of trade secrecy is still in an early stage of development in India, clear standards on this point are evolving. For example in *American Express Bank Ltd* v. *Priya Puri*, the court considered the question of whether or not a list of customers could qualify as a trade secret.[89] The plaintiff was a wealth-management company seeking an injunction to restrain a departing employee from disclosing the identities of their customers to the former employee's new employer. Even though the former employee's engagement contract specifically defined customer identities as trade secrets not to be disclosed upon termination or departure, the court refused to grant the injunction, reasoning that to do so would act as an unreasonable restraint on employee mobility. The court explained that although banks owe their customers a duty of confidentiality, this duty does not empower the bank with a protectable trade secret because finding otherwise could impair the ability of customers to take their business elsewhere.

9.117 Although the foregoing case is likely to upset some businesses, it is not unlike US case decisions where customer lists have been found to be trade secrets in many circumstances, but not all. Whether customer lists are trade secrets in the United States often depends upon the specific content of the customer list and whether the information that is contained therein is generally known or readily ascertainable. Or, as in the foregoing example, there may be a public, employee or customer interest in the use and dissemination of the customer list that is paramount. In India, this must be understood against the backdrop of the constitutional guarantee of freedom to practise any profession or carry on any occupation, subject only to reasonable government regulation.[90] This guarantee is discussed in greater detail, below.

9.118 Like the law of the United States, the law of India apparently makes a distinction between information that qualifies for trade secret protection and other forms of confidential information. However, perhaps because India borrows trade secret principles from both England (which focuses on confidential information) and the United States (which focuses on trade secrets), the line between trade secrets and confidential information can blur easily and the terms are sometimes used interchangeably.

89 (2006) IIILLJ 540 Del.

90 Indian Constitution, art. 19.

9.119 In India, confidential information is defined as 'valuable or sensitive information received in confidence which can neither be disclosed nor used for any purpose other than that for which the information was received unless prior consent of the owner is obtained'.[91] In general, the term 'confidential information' is usually applied to 'a single or ephemeral event in the conduct of a business, whereas a trade secret may be a process, device for continuous use or compilation of data that is used repeatedly'.[92] In the United States, confidential information not otherwise meeting the definition of a trade secret is generally not protected in the absence of a contract. Thus, this is one area of current Indian law that may provide marginally greater protection than is available under US law.

9.120 While the theoretical scope and definition of trade secrets under Indian law are consistent (and perhaps somewhat broader) than US law, in practice trade secret rights in India are significantly limited due to a narrow conception of misappropriation under Indian law and the effects of other legal principles, such as the importance of employee mobility. Just as there is no statutory law defining a trade secret in India, there is no enacted definition of misappropriation either.

9.121 In keeping with the common law origins of trade secret claims in the United Kingdom and the United States, and the language of Article 39.1 of the TRIPS Agreement, the definition of misappropriation in India depends upon what behaviour is considered 'unfair' or 'contrary to honest business practices'. As trade secret law in India has developed thus far, unfairness typically equates with breach of a duty of confidentiality and, in fact, on this issue Indian courts often cite the English case of *Coco* v. *A.N. Clark Engineers Ltd,* discussed above.[93] As in the United Kingdom, such a duty of confidence may arise from an express agreement or be implied from the circumstances.[94] However this later theory is typically limited in India by the condition that a duty of confidence can only be enforced by a foreign plaintiff against a party that is either a fiduciary or in an employee-employer relationship with the foreign plaintiff.[95] These limits are discussed in greater depth in the section on employment relationships, below.

9.122 India has been criticized for not recognizing a cause of action for trade secret misappropriation based upon the acquisition of trade secrets by improper means. Unfortunately, in this regard, the language of footnote 10 of the TRIPS

---

91 Taneja and Bhardwaj, n. 85 above, at 15.
92 *Ibid.*
93 [1969] RPC 41.
94 *John Richard Brady* v. *Chemical Process Equipments P. Ltd* (2003) Bom. CR 563.
95 Baldia, n. 85 above, at 10.

Agreement does explicitly define improper means in the same way that it is defined in the UTSA. It only states that a 'manner contrary to honest business practices' means 'at least practices such as breach of contract, breach of confidence, and inducement to breach'. The scope of Indian law, as just described, appears consistent with this definition. However, under the common law process of law, the Indian courts can be encouraged to recognize a broader definition of misappropriation, citing US law. Also, where the alleged misappropriation involves the acquisition of trade secrets through copying, a claim for relief may be brought under India's Copyright Act.[96]

9.123 Despite the lack of case precedent to help define 'improper means', precedent does exist under Indian law to establish that reverse engineering and independent development are proper means to acquire information, including trade secrets. This is consistent with the understanding that was reached during the TRIPS negotiations, discussed in Chapter 2, although words to that effect are not included in Article 39 of the TRIPS Agreement.

9.124 Based upon the foregoing, in India (as elsewhere) the best practice is for the owner of a purported trade secret to protect its information by express written contract. However, non-disclosure agreements and other contractual means of protection are subject to strict limitations of reasonableness and must not violate the constitutional fundamental right of individuals to pursue a livelihood.

C. Trade secret issues in employment relationships

9.125 In Chapter 3, which discussed US trade secret principles, it was noted that the protection of trade secrets in each of the US states may differ somewhat due to the extent that an individual state is more or less solicitous toward the interests of employees and protective of employee mobility and free competition. The same can be said of individual sovereign nations, particularly a democratic socialist republic like India. For various reasons due to its history and values and the circumstances surrounding its independence, India (not unlike Japan) felt it was important to build various labour and employment protections into its Constitution. Thus, the right to pursue a livelihood is a fundamental right in India[97] and agreements that interfere with that right are highly suspect.

96 See *Puneet Industrial Control* v. *Classic Electronic* (1997) Arb. LR 195 Del. 9 and *Burlington Home* v. *Rajneesh Chibber* (1999) PTC 36 (Del).

97 Bloomberg BNA, *Restrictive Covenants and Trade Secrets in Employment Law: An International Survey* (2011), 'India', para. 16.I.A .

9.126 Consistent with the foregoing, section 27 of the Indian Contract Act provides that: 'Every agreement by which anyone is restrained from exercising a legal profession, trade or business of any kind, is to that extent void'. This is similar to the statutory law of California (which dates from 1872) that holds non-compete agreements void *ab initio* unless meeting a statutory exception.[98] Like California law, the Indian Contract Act includes an exception for situations involving the sale of the goodwill of a business; however, even these agreements are subject to requirements of reasonableness.

9.127 Despite the foregoing, Indian law generally recognizes that employees owe a duty of loyalty to their employer which includes an obligation of confidentiality.[99] Moreover, over time, the severity of section 27 law has been relaxed with respect to non-compete agreements between employers and employees.[100] Thus, although the statute does not make an express exception for contractual restrictions that are designed to protect trade secrets, case law exists in India that would allow such agreements between an employer and an employee as long as the agreement is otherwise reasonable. Additionally, non-disclosure and confidentiality agreements between an employer and an employee are also generally enforceable as long as they are reasonable.

9.128 Post-termination restrictions are viewed with suspicion by Indian courts. Thus, non-compete agreements that apply post-employment are presumed invalid with no regard given for reasonableness. Post-employment non-disclosure agreements are enforceable so long as they are reasonable, limited in time and scope and the employer can prove that the information in question is confidential and proprietary.[101]

9.129 With respect to the ownership of employee-created inventions and information, the law of India seems similar to, but less developed than, the law in the United States. Generally, the ownership (or control) of such inventions and information is a matter of contract.[102] Thus, the best practice in India is to obtain a written invention assignment agreement, but care should be exercised to make it reasonable, particularly with respect to any post-employment activities. In cases where no such agreement is obtained, there are theories under which an employer can obtain rights in employee-created inventions or

98 Contract Act, No. 9 of 1872, India Code, s. 27: 'Every agreement by which any one is restrained from exercising a lawful profession, trade or business of any kind, is to that extent void'.

99 *Bombay Dyeing and Manufacturing Co. Ltd* v. *Mehar Karan Singh*, n. 88 above.

100 Hemant Singh, *Protection of Trade Secrets through IP and Unfair Competition Law*, AIPPI Report Q215, India 6 (2010).

101 *Ibid*. para. 16.B.I.B.4.A.

102 Singh, n. 100 above.

information, including applicable provisions of the Indian Copyright Act, the assertion of an implied agreement and the assertion of an implied duty of confidence.

9.130 With respect to the implied duty of confidence often owed by employees, Indian law recognizes the so-called 'springboard doctrine', a concept first developed in courts of England and Wales (discussed above) to address the perceived unfairness of former employees using confidential information they took from a former employer to compete with a former employer. The springboard doctrine applies in situations where, as a matter of equity, 'courts are bound to restrain someone who has come into the possession of certain information and is unlawfully using it as a "springboard" to derive economic or commercial gain at the detriment of the rightful owner'.[103] Therefore, the preferred remedy in such cases is usually injunctive relief tailored to deprive wrongdoers of the lead-time advantage of their unlawful acts.[104] This 'springboard injunction' must be sought and obtained while the wrongdoer is still enjoying an unlawful advantage because the purpose of the relief is to restore the parties to the position they would have been in had it not been for the wrongdoer's misconduct and not to punish the defendant.

D. Trade secrets in business relationships

9.131 Given its long legal tradition and commercial history, India has a well-developed body of contract and commercial law which generally enforces contracts that are entered into between business interests. This includes reasonable confidentiality agreements and non-compete agreements. Because business-to-business agreements are less likely to implicate the fundamental right to pursue one's calling, they are apt to be more enforceable than agreements entered into between a business and its employees. However, general competition rules (antitrust rules in US parlance) will apply, as will the provisions of section 27 of the Contract Act, discussed below.

9.132 Generally, contract law in India is based upon the Indian Contract Act 1872 (Act No. 9 of 1872) as interpreted and applied by Indian courts. Competition principals are governed by the Competition Act 2002, as amended, which has recently begun to be enforced with more vigour. Among other things, it prohibits 'agreement[s] in respect of production, supply, distribution, storage,

103 Taneja and Bhardwaj, n. 85 above, at 14.

104 *Ibid*. (quoting *QBE Management* v. *Dymoke* [2012] EWHC 80 (QB) (UK)).

acquisition or control of goods or provision of services, which causes or is likely to cause an appreciable adverse effect on competition within India'.[105]

9.133 Theories of liability against third parties who come to possess confidential information, not directly from the information owner but through an individual or company that is under a duty of confidentiality, are not well developed in India, despite the fact that footnote 10 of the TRIPS Agreement requires such protection. However, *dicta* from one recent case suggest this may be changing.[106]

9.134 To the chagrin of many businesses that wish to conduct business in India, India has long regulated technology transfer agreements related to inbound technology, including license agreements of the type discussed in Chapter 4. Based upon this regulation, it has been noted that Coca-Cola refused to conduct business in India for a period of time because to do so would have required it to disclose its trade secrets and allow them to be sublicensed.[107] Under pressure from the United States and other countries, these regulations have been relaxed, but some technology transfer agreements will still be reviewed by governmental authorities.

E. Criminal consequences for trade secret misappropriation

9.135 There are no specific criminal laws in India that prohibit the misappropriation of trade secrets, per se. However, as in the United Kingdom, there are a number of criminal laws that prohibit behaviour that often accompanies trade secret misappropriation, such as theft, fraud, receipt of stolen property, breach of trust and criminal misappropriation.[108] Other acts criminalize computer hacking and other forms of data theft.[109]

9.136 The apparent difficulty with applying these other criminal laws to trade secret misappropriation claims is India's narrow conception of property which holds that 'information, as such' is not property. For instance, although section 405 of the Indian Penal Code defines a 'criminal breach of trust', it is recognized that the reference to 'property' in that statute refers to immovable and movable property, and does not apply to intangible property like trade secrets.

---

105 Competition Act of India, ch. II, s. 3(1), available at www.cci.gov.in/images/media/competition_act/act2002.pdf?phpMyAdmin=QuqXb-8V2yTtoq617iR6-k2VA8d.

106 *AIA Engineering Pvt Ltd* v. *Bharat Sand and others*, AIR 2007 Gujarat (NOC) 1456.

107 *Coca-Cola Bottling Co. of Shreveport, Inc.* v. *Coca-Cola Co.*, 107 FRD 288, 294 (D Del. 1985).

108 *Halsbury's Laws of India*, paras 105.1671 *et seq.*, 105.1753–6 and 1285.369.

109 Pravin Anand, *Trade Secrets Throughout the World: India*, vol. 2, para. 19:2.

F. Litigating trade secret disputes

9.137 Trade secret owners who believe that their trade secrets have been misappropriated can bring a civil action in the appropriate district court and, as noted above, plead a number of common law theories of recovery. The Code of Civil Procedure 1908, as amended, governs the litigation process in India.[110] Generally, civil litigation (including trade secret litigation) is commenced with the filing of a written complaint. The case then proceeds through service upon the defendant, a pleading stage, a discovery stage and, ultimately, a trial conducted before a judge, as there are no jury trials in India. Due to a number of factors, the resolution of cases in India is very slow and judicial corruption has been reported.

9.138 The good news for litigants, at least those who prefer the US-style of litigation, is that Indian courts are empowered to issue orders concerning discovery, including answers to interrogatories and the production of documents.[111] Also, witnesses can be summoned to give evidence and produce documents and other material objects at trial, and the courts have the power to compel compliance with issued summons. The Code of Civil Procedure also sets forth numerous provisions empowering the courts to enforce judgments and decrees.

9.139 The fact that discovery can be ordered 'as reasonable', and the district courts of India have broad powers to enter other orders as necessary, means that protective orders and *in camera* hearings can be requested to protect trade secrets. However, as in England and Wales, no specific provision of the Code of Civil Procedure requires the issuance of protective orders in trade secret cases or the sealing of court records.

9.140 Without a detailed statute like the UTSA, the remedies that are available in India for trade secret misappropriation depend upon the cause of action upon which such claims are based, be they contract, tort, unfair competition, copyright or equitable. They may also include preliminary and permanent injunctions, Anton Piller orders (aka civil seizure orders, discussed in the UK section above), monetary damages and orders that require the trade secrets to be turned over.

9.141 The Code of Civil Procedure of India (Act No. 5 of 1908), section 94(c) provides that a court may 'grant a temporary injunction and in case of disobedience commit the person guilty thereof to the civil prison and order that

110 Vinay Vaish *et al.*, n. 82 above.
111 *Ibid*. para. 5.2.

his property be attached and sold'. Thus, Indian courts have the power to grant preliminary and permanent injunctive relief, and will do so upon a proper showing.[112]

112 See *Escorts Construction* v. *Action Construction* (1999) PTC 36 (Del.).

10

COUNTRY OVERVIEWS: CIVIL LAW COUNTRIES

I. INTRODUCTION TO CIVIL LAW COUNTRIES

10.01 As previously discussed in Chapter 8, most countries of the world, approximately 150, follow the civil law tradition whereby law is made primarily through the adoption and frequent re-evaluation and amendment of written codes. Thus, the primary source of law in civil law countries is the written code, with judicial decisions having little or no precedential value.

10.02 In this chapter the legal traditions and trade secret laws of four civil law countries are discussed: Brazil, China, Japan and Mexico. China and Japan were selected because of their positions as significant centres of trade and as two of the top three economies in the world. Brazil is featured as one of the so-called BRIC (Brazil, Russia, China and India) countries due to its position as a country with an expanding economic base and because of the importance of

featuring a country from the southern hemisphere. Mexico is included because of its trade relationship with the United States and its membership in the North American Free Trade Agreement (NAFTA). Although members of the WTO since its inception, as developing countries, Brazil and Mexico were not required to be in full compliance with the TRIPS Agreement until 1 January 2000. China joined the WTO in December of 2001.

10.03 In light of the possible approval of the proposed EU Trade Secret Directive (see Appendices 1 and 2), it was decided not to discuss other large civil law countries within the European Union (such as Germany, France, Spain and Sweden) since their existing laws may be amended to comply with the Directive. However, many of the general observations about civil law countries that are made in this chapter apply to those countries as well. Additionally, the discussion of the EU Directive in Appendix 1 of this book provides an overview of what may become the trade secret principles for all EU countries.

10.04 Other civil law countries include: all members of the EU except the United Kingdom and Ireland, as well as the countries of Argentina, Egypt, Russia, South Africa, Switzerland, Taiwan, Turkey and Vietnam. The Canadian province of Québec and the US state of Louisiana also follow the civil law tradition.

II. BRAZIL

A. Overview of the legal system

10.05 Brazil has a history similar to Mexico with a rich indigenous culture and a story of conquests and political turmoil, but whereas the Mexican legal system (as discussed below) was largely influenced by over 300 years of Spanish rule, the Brazilian legal system was influenced by Portuguese legal traditions. This is due to the fact that Brazil was a colony of Portugal from 1500 to 1822, roughly the same period of time that Spain ruled Mexico.

10.06 In September 1822, Brazil declared its independence from Portugal. There followed a series of different governments beginning with the Kingdom and Empire of Brazil and followed by the Republic of Brazil, a dictatorship and periods of military rule. The current form of government, with a democratically elected President, has been in place since the late 1980s, meaning that as of 2015 there are roughly 30 years of development of laws and legal principles under the current system.

10.07 Brazil is a geographically large country, with its trading centres located in disparate parts of the country. Brazil's economic evolution over the last decade has led to its recognition as a significant economic force.[1] It is the leading nation among Latin American economies and has attracted billions of dollars in foreign investment from corporations and governments.[2] Brazil has become one of the United States' top trading partners and estimates are that it will soon become the world's fifth-largest economy (larger than the economies of the United Kingdom and France).[3]

10.08 Brazil has a federal system of government with a democratically elected federal legislature and an elected President in the executive branch. The legislative branch is known as the National Congress and includes the Federal Senate and the Chamber of Deputies. It is believed by some that this political structure fosters corruption. In part, this is because the system allows a large number of political parties to participate in elections and these parties often seek to attract voters through new benefits, government jobs and public contracts. Despite the recent economic success of Brazil, it is believed that these issues with Brazil's regulatory and legal framework tend to impede foreign investment in the country. Thus, among the many reforms that have been instituted in Brazil to encourage foreign investment has been reform of the judicial system.

10.09 Brazil's Constitution serves as the foundation for the country's legal system.[4] The Constitution was adopted in 1988 following 21 years of a military dictatorship and has subsequently been amended numerous times. In addition to ensuring that many individual rights would be guaranteed, the Constitution also provides for economic rights. For instance, article 5 of the Federal Constitution guarantees all persons the right to property, including intellectual property. However, observers have noted that there is a gap between the rights and protections as written in the law and the practice on the ground in Brazil.[5]

10.10 The judicial branch of Brazil is composed of the Supreme Federal Tribunal, the Superior Court of Justice, regional federal courts and judges, labour courts, electoral courts, military courts and state and federal district courts. The 1988 Constitution created an elaborate system of judicial review. It combines a decentralized form of review similar to that in the United States with a more

1 See Enrique R. Carrasco and Sean Williams, 'Emerging Economies After the Global Financial Crisis: The Case of Brazil' (2012) 33 *NW J Int'l L and Bus.* 81.

2 See Grant R. Garber, 'Noncompete Clauses: Employee Mobility, Innovation Ecosystems, and Multinational R&D Offshoring' (2013) 28 *Berkeley Tech. LJ* 1079, 1092–3.

3 See 'Brazil Takes Off', *The Economist*, 14 November 2009, p. 15.

4 Constituição da República Federativa do Brasil (Constitution) (CF).

5 See e.g., Keith S. Rosenn, 'Procedural Protection of Constitutional Rights in Brazil' (2011) 59 *Am. J Comp. L* 1009, 1010; Augusto Zimmerman, 'Constitutional Rights in Brazil: A Legal Fiction?' (2007) 14 *eLaw J* 28, 55.

centralized and abstract form of review modeled after some European countries. The Supreme Federal Tribunal is the highest court and Tribunals of Justice are the highest state courts. The Supreme Federal Tribunal decides both constitutional and non-constitutional matters, many of which it has already previously decided. That is because, unlike the US Supreme Court, it does not have a writ of certiorari mechanism through which it selects cases or a *stare decisis* doctrine to eliminate the re-litigation of settled issues.

10.11 Brazil's judiciary is reputed to be slow and inefficient. Its courts have very large caseloads. The Judicial Reform Amendment[6] was meant to reform the judiciary and it provides, in part, that decisions rendered by the Supreme Federal Tribunal (with concurrence by two-thirds of the 11 justices sitting *en banc*) will be binding precedent on the entire judiciary as well as on federal, state and county public administration.[7] Motivating this law was the need to encourage consistency and efficiency. The hope was that it would reduce the incidence of courts having to decide the same issues repeatedly. Nevertheless, the vast majority of the courts' caseloads include questions that have already been decided.[8]

10.12 While the time-frame for the resolution of civil actions in Brazil varies, in general, it takes years to resolve a dispute. Not only does it take several years in state courts and superior courts for rulings to be issued, but the losing party often appeals. Brazilian law permits appeals against every intermediate decision issued by a judge. This further contributes to the lengthy delays to obtain final resolution of a case.

10.13 Brazil has agreed to protect intellectual property rights (IPRs) since it joined the Paris Convention in 1883. A few years later, in 1887, it enacted its first intellectual property law. It joined the Berne Convention in 1922. In 1970, the National Industrial Property Institute was created. This Institute serves as the Brazilian Patent and Trademark Office. As such, it is responsible for registration and protection of intellectual property in Brazil.

10.14 Brazil is also a signatory to the WTO Agreement effective 1 January 1995 and was required to be in full compliance with the TRIPS Agreement by 1 January 2000. In May 1996, the Brazilian National Congress enacted a new Industrial Property Law (Law 9.279) which was meant to bring Brazilian law into

6 CF, amendment No. 45 (8 December 2004) (Braz.).

7 See Rosenn, n. 5 above, at 1035.

8 Keith S. Rosenn, 'Judicial Review in Brazil: Developments Under the 1980s Constitution' (2000) 7 *Sw J L and Trade Am.* 291, 313.

compliance with the TRIPS Agreement. Two other bodies of statutory law governing intellectual property were subsequently adopted. These are the Copyright Law (Law 9.610) and the Software Law (Law 9.609).[9]

B. Contours of trade secret protection

10.15 Unlike the United States and a number of other countries, Brazil has not established a specific civil cause of action for trade secret misappropriation. However, the kinds of conduct implicated in trade secret cases, such as breaches of confidentiality and espionage, fall under criminal law in Brazil (specifically the crime of unfair competition) and may be prosecuted. Thus, trade secret protection is part of the broader criminal statutory rules governing unfair competition, rather than having specifically delineated rights under its intellectual property legal framework, as is the case with respect to patents, trademarks, copyrights and geographical indications. Further contributing to the lack of clarity of Brazilian trade secret law is the fact that there have been very few trade secret cases ruled on by the courts. Accordingly, there is not a rich and informative body of law from which to ascertain the true nature of trade secret protection in Brazil.

10.16 The Industrial Property Law (IPL) of Brazil became effective on 15 May 1997. Title V of the IPL addresses 'crimes against industrial property'. Chapter VI (article 195) of that title is titled 'Crimes of Unfair Competition' and this is the part of the law that appears to deal with trade secrets. More specifically, article 195(XI) and (XII) of the IPL makes it an act of unfair competition if one:

> divulges, exploits, or utilizes, without authorization, confidential knowledge, information, or data that could be used in industry, commerce, or rendering of services, other than that which is of public knowledge, or that would be evident to a technician versed in the subject, to which he gained access by means of a contractual or employment relationship, even after the termination of the contract.

The prohibition in subsection XII applies when the information is obtained 'by illicit means or when access was gained through fraud'.

10.17 Note that although the section as translated does not explicitly define trade secrecy, some of the usual key components required for protection of confidential (trade secret) information under the TRIPS Agreement appear to be present: it must be secret and, impliedly, have value. It protects confidential

9 Some other statutes that also implicate intellectual property rights are art. 5 of the Brazilian Constitution, the Consumer Code (Law 8.078), and the law governing corporate names (Law 8.934).

knowledge that is capable of being utilized in industry, commerce or the supplying of services and it explicitly excludes information which is in the public domain or known to experts in the field. However, there is no specific reference in the language of the IPL to the requirement that the owner must have taken reasonable steps to protect the information.

10.18 Apparently, any information can be protectable as a trade secret if it provides a competitive advantage to its owner.[10] This includes such information as client lists, donor lists, marketing strategies, manufacturing processes and organizational structures. Also, both commercial and technical information can be protected.

10.19 The categories of wrongdoers that Brazilian law reaches are somewhat unclear. Subsection XI makes specific reference only to information gained in a contractual or employment relationship and thus appears to prohibit misappropriation of trade secrets in breach of a duty of confidentiality. Subsection XII covers misappropriation by 'illicit means' and fraud, but it is unclear whether it would include other wrongful acts, such as those that may be included under industrial espionage. More broadly, it is unclear whether Brazilian law prohibits all of the behaviours listed in footnote 10 of the TRIPS Agreement.

10.20 The general provisions of the IPL which relate to all of the titles (not just the unfair competition chapter) provide that 'independently of the criminal action, the aggrieved party may bring any civil suits he considers as appropriate pursuant to the Civil Procedure Code'.[11] In turn, the Civil Code provides that any person who violates the rights of another person and causes damage to them, even though the damage is exclusively moral, commits an illicit act and is required to repair the damage.[12] Similar to the Civil Code, there is also a Code of Civil Procedure that protects trade secrets by protecting parties and witnesses from having to testify to any facts that are considered secret. It also provides that a judge may order a search and seizure of persons or things as an available legal remedy.[13] One final avenue for civil relief is under the Labour Law which provides that violation of trade secrets is just cause for termination of an employee by an employer.[14] Accordingly, while there is no specific civil provision on trade secrets, these various civil options, read broadly, may be applicable

10 See TJES –AI: 12049000149, ES 12049000149, Relator: Carlos Roberto Mignone, 17 April 2007, Quarta Câmara Cível, 31 May 2007 (Braz.)

11 Lei No. 9.279, tit. VII, art. 207, 14 May 1996, DO 15 May 1996 (Braz.) (Industrial Property Law of Brazil).

12 Codigo Civil, art. 229(I) (Braz.).

13 Lei No. 5.869, 11 January 1973, DO 17 January 1973 (Braz.).

14 Consolidacao das Leis do Trabalho (CLT), art. 482 (Braz.).

and provide a civil option for companies that are victims of trade secret misappropriation.

C. Trade secrets in employment relationships

10.21 Obligations to protect trade secrets are enforceable against current and former employees as well as business partners whether those obligations are express or implied.[15] Brazilian law recognizes agreements between employers and employees providing for the confidentiality of secret information. Additionally, a breach of duty is specifically defined to include duties arising from a contractual or employment relationship. Both employees and fiduciaries have a duty not to disclose an employer's trade secrets, even without a written contract.

10.22 The labour laws in Brazil address obligations of secrecy between an employee and employer and permit an employer to lay off an employee who has breached its obligations to an employer.[16] Article 482 of the Consolidated Labour Laws of Brazil provides that 'violation of the enterprise's secrets' shall constitute just cause permitting the employer to dismiss the employee without notice.

10.23 Under Brazilian law, employees are free to work for a competitor as long as they do not breach any duties owed to the previous employer.[17] They may also use and develop their professional skills and knowledge even if some of it was acquired while serving their employer. Nonetheless, non-competition agreements are generally allowed but will be reviewed on a case-by-case basis to determine reasonableness. As one commentator has observed, while the non-compete law in Brazil is not as developed as in countries like China or India, it does seem to give deference to employer interests in protecting trade secrets.[18]

10.24 While non-competition provisions are generally enforceable in Brazil, they must not violate competition law.[19] They must be related to the protection of trade secrets, be limited in duration and geographic scope and provide compensation to the former employee during the period of the non-compete agreement. Brazilian labour courts in determining reasonableness will review the conditions imposed during the non-competition period, such as the territory covered, limitation of time, financial compensation and the core business affected. To boost the reasonableness of such agreements, it is generally advisable that non-compete agreements in Brazil provide for compensation to

15 See Jose Antonio B.L. Faria Correa, *Trade Secrets Throughout the World: Brazil* (2013), vol. 1, paras 5:11–5:12.
16 See CLT, art. 482(g) (Braz.).
17 See generally CF tit. II, art. 5 (Braz.).
18 See Garber, n. 2 above, at 1107–8.
19 See Lei No. 12.529, 30 November 2011, Diario Oficial da Uniao, 1 December 2011 (Braz.).

the former employee. Accordingly, non-compete provisions in employment contracts should be drafted cautiously.

10.25 As in the United States, the ownership of employee inventions in Brazil is governed by the circumstances and the nature of the relationship under which the invention came into being. Inventions conceived by employees or consultants belong exclusively to the employer if the employee has signed an express inventive agreement or served an implicit inventive function.[20] If the employee does not have an express or implied inventive function, but conceived the invention using the employer's facilities, any rights are to be shared equally and the employer is entitled to obtain an exclusive licence to the invention. When neither of these circumstances are met, such that an employee conceives of an invention that has no relation to any agreements with the employer or having used the employer's facilities, the invention belongs exclusively to the employee.

D. Trade secrets in business relationships

10.26 As noted above in the context of employees, confidentiality agreements are valid and enforceable in Brazil. The same is true for business-to-business relationships. The agreement can be written or implied from the circumstances, including from the nature of the relationship between business partners.[21] Also, liquidated damages for disclosure can be provided for in such contracts and will generally be enforced.

10.27 With respect to licensing, Brazil has policies that reflect its concern that private agreements may be used to hamper technology transfer and the diffusion of knowledge. Thus, licensing agreements involving trade secrets, while not prohibited by law, are viewed with disfavour by Brazil's National Industrial Property Institute (INPI) which is also the Brazilian Patent and Trademark Office (BPTO). Significantly for companies doing business in Brazil, agreements concerning the licensing of intellectual property rights must be registered with the INPI for approval.[22]

10.28 INPI views unpatented technology as inappropriate subject matter for a license agreement and treats it more as the equivalent of a sales transaction. Because restrictions on the use or disclosure of secret information after termination of an underlying license agreement is inconsistent with a sales transaction, INPI has

20 See Industrial Property Law of Brazil, art. 88.
21 See *ibid.* art. 195(XI).
22 See *ibid.* art. 211.

taken the position that secrecy obligations should last no more than 19 years starting from the disclosure of each piece of information. As such, it does not accept confidentiality provisions in perpetuity since the confidentiality obligation cannot extend beyond the term of a valid patent.[23]

10.29 Because INPI disfavours licensing of non-patented technology such as trade secrets, the agency has placed restrictions on trade secret licenses. Some of these restrictions include not authorizing clauses that limit the use of know-how (even after the termination of the agreement), that limit use of information after expiration of an agreement and unlimited confidentiality terms. This is consistent with the view of Brazil that technology that is not protected by a patent can only be transferred to a Brazilian party rather than licensed. This means that trade secrets are easier to assign than to license.

10.30 The agency's authority to restrict the licensing of trade secrets has been contested in courts, but its power to review and evaluate these agreements has been upheld. However, INPI's role has been narrowed by article 240 of the 1996 IPL which limits its authority to determining whether formal requirements imposed by statute have been met and to enforcing industrial property regulations at the national level. Thus, INPI no longer has the authority to reject license agreements that do not conform with other policies, including its own.

10.31 While there is no maximum royalty that can be imposed in a trade secret license agreement, INPI may refuse to approve agreements that contain a royalty that is considered to be higher than those charged by the licensor in other similar international transactions. However, technology transfer agreements between a foreign parent company and a Brazilian subsidiary are subject to a limit on royalties.[24] The maximum allowed royalty formula is equivalent to the corresponding ceiling for tax deduction as set by the Ministry for Financial Affairs, which ranges between 1 and 5 per cent of the net sales price for the contracted products. Accordingly, INPI will not accept explicit lump sum license payments, since all amounts to be paid should be based on product sales.

10.32 The foregoing policies create obstacles for enforcing trade secret rights in Brazil and for entering into appropriately effective agreements with other companies. While the trade secret owner may protect trade secrets against espionage and a breach of duty by employees and business partners, the same does not apply to licensing. This creates a trap for the unwary when entering into these kinds of agreements.

---

23 See Faria Correa, n. 15 above, para. 5:14.

24 See *ibid.*

E. Criminal consequences for trade secret misappropriation

10.33 As noted earlier, protection for trade secrets in Brazil is primarily provided under the criminal law. Article 195(XI) and (XII) of the 1996 Industrial Property Law defines the crime of unfair competition in Brazil. Subsection XI provides that anyone who 'divulges, exploits, or utilizes, without authorization, confidential knowledge, information, or data that could be used in industry … other than that which is public knowledge … to which he gained access by means of a contractual or employment relationship, even after the termination of the contract or employment' is guilty of unfair competition. Furthermore, subsection XII adds that divulging, exploiting or utilizing the confidential information described in subsection XI 'when obtained by illicit means or when access was gained through fraud' is also a crime.

10.34 Based upon the foregoing, misappropriation of trade secrets occurs through unauthorized disclosure, unauthorized exploitation and unauthorized use of trade secret information. The offence may be committed by employees or persons having a contractual relationship with the trade secret owner, even after the relationship is over. A third party may also be guilty if a trade secret was obtained by fraud or other illegal means. Accordingly, the kinds of offences that are covered under the criminal law of Brazil are very similar to those covered under civil laws in the United States. Significantly, however, criminal penalties for trade secret misappropriation are relatively light, ranging from three months to one year in prison or a fine and are imposed on individuals only.

F. Litigating trade secret disputes

10.35 In Brazil, a company that has suffered harm as a result of trade secret misappropriation may file a criminal complaint. Criminal actions against an individual for trade secret misappropriation (unauthorized disclosure) are heard by state judges and this is the primary way to redress trade secret harm. In addition, civil lawsuits can be filed for damages in a related action, as provided in article 207 of the 1996 Industrial Property Law. It provides that an injured party may claim damages arising out of the criminal act for both moral and material damage. More generally, the Brazilian Civil Code provides that any person who violates the rights of another person and causes damage to them, even though the damage is exclusively moral, commits an illicit act and is required to repair the damage.[25] One final avenue for civil relief is under the

25 Codigo Civil, arts 186, 927 (Braz.).

Labour Law, which provides that violation of trade secrets is just cause for termination of an employee by their employer.[26]

10.36 In unfair competition cases, material damage has to be proven by the plaintiff, but moral damage is presumed by law. While traditionally Brazilian courts tend to award only actual damages, article 210 of the IPL requires courts to consider other factors in intellectual property infringement and unfair competition cases. These include, for instance, the financial and other benefits that the injured party would have obtained without the infringement, the financial and other benefits actually obtained by the infringer or compensation that the infringer would likely have paid to the owner of the industrial property as a license fee for use of the property right.

10.37 Unlike in the United States, but as is common in civil law countries, pretrial discovery in Brazil is mostly documentary and conducted under the supervision of a judge. Accordingly, the parties may not initiate pretrial discovery and may not compel one another to produce evidence without the court's participation. However, during the evidentiary phase of a case, orders can be obtained to require the opposing party to produce documents in its possession. The requesting party must detail the documents it seeks and the facts relevant to those documents. The opposing party may then dispute the request. Also, both the criminal and civil laws provide for preliminary search and seizure actions to collect evidence.[27]

10.38 There are provisions for protecting trade secrets during litigation in Brazil, including review of materials *in camera.* Article 206 of the IPL provides that '[i]n the event that information disclosed in court … is characterized as confidential, whether industrial or trade secret, the judge shall order that the proceedings be held in camera, and the other party shall be prohibited from using such information for other purposes'.[28] There is also a special provision for infringement actions involving software (such as source code) which requires that they be tried *in camera*.[29]

10.39 Pursuant to the Civil Procedure Code (CPC), a court may enter a preliminary seizure order to collect any confidential material stolen from a plaintiff if evidence is presented that the plaintiff has a right to the materials and that the defendant's actions would cause irreparable injury. The trial judge may also

26 CLT, art. 482 (Braz.).
27 Civil Procedure Code (CPC), art. 273 (Braz.); CPC, art. 461 (Braz.); CPP, art. 525 (Braz.).
28 Industrial Property Law of Brazil, art. 206.
29 Lei No. 9.609/98, 19 February 1998 (Braz.).

award an *ex parte* injunction in circumstances where notice of the hearing would frustrate the legal remedy. Temporary restraining orders can also be issued, and whenever injunctions are imposed in a preliminary fashion the complainant must file a lawsuit within 30 days of its issuance.[30]

10.40 Although injunctions are available in Brazil, it does not appear that they can be obtained as quickly as in the United States. Accordingly, they are not necessarily a meaningful option when trying to prevent the public disclosure of trade secrets. In part, this is due to the slowness with which cases tend to move through the Brazilian court system. There is a procedure known as a 'tutela antecipada' which allows judges to preserve the position of a wronged party through what appears to be preliminary injunctive relief. While this is used with some frequency in trademark and patent cases, it is reportedly not often requested or granted in trade secret cases.[31]

10.41 Third parties may be liable for using or disclosing trade secrets, provided that they have knowledge that the trade secret was disclosed in breach of a duty or that it was otherwise misappropriated. While there does not appear to be case law on this issue in Brazil, it is believed that a gross negligence standard as provided in Article 39.2 TRIPS, applies: 'businessmen are supposed to know, or to take the necessary precautions within their companies to be aware of which information is or has the potential to be a trade secret, under reasonable situations'.[32] Without such knowledge an innocent party is not likely to be held liable.

III. CHINA

A. Overview of the legal system

10.42 To understand the legal system of mainland China today requires an appreciation of the history and culture of China and the many influences that shape that system. Compared to the United Kingdom and the United States, China is a relative newcomer in the development of modern laws and associated legal systems, with the process dating from the formation of the Chinese Republic in the early 1910s. This is not to say, of course, that China was a lawless society before that date, as traditional Chinese law had developed and was in use in

30 Faria Correa, n. 15 above, para. 5.13.

31 See Roger M. Sherwood, 'Trade Secret Protection: Help for a Treacherous Journey' (2008) 48 *Washburn LJ* 67, 72.

32 See Agreement on Trade-Related Aspects of Intellectual Property Rights, Annex 1C, 'Legal Instruments: Results of the Uruguay Round', vol. 31, art. 39.2, n. 10, 33 ILM 81 (1994).

China until the early twentieth century, including principles of trade secret protection. However, for various reasons, including the influences of the loss of the Opium War and foreign trade in the latter part of the Qing Dynasties (1644–1912), the Chinese government was in turmoil for much of the twentieth century.

10.43 Although the history of China is very long (dating from ancient times) and complex, the applicable systems of government can be broken into three periods. Early in its history, until 1912, China was ruled by various dynasties that developed traditional Chinese law. Importantly from a current cultural perspective, this body of law was heavily influenced by Chinese legalism (marked by strict adherence to written laws) and Confucianism (marked by ethical principles which focus on improvement of self and the importance of family and, most important, notions of discretionary exercise of power). In 1912, the Republic of China was formed to replace the last ruling dynasty, but for various reasons it was not successful in establishing a strong unified government and ultimately it was overthrown by the People's Liberation Army. This led to the creation of the People's Republic of China (PRC) in 1949.

10.44 The foregoing history helps explain the underpinnings of modern Chinese society and law. As one commentator has noted:

> As you study the law of China and its economic policies, [a short history of China] should give you some hint as to how China currently conducts itself in matters of political, economic, and foreign relations. Much of these policies derive from the experiences of China during the late Qing Dynasty under foreign rule and its own internal struggles for a unified country in the modern world. China's first encounters with international business and trade led to foreign domination and imperialist demands backed by the point of a gun.[33]

Initially, from 1949 until economic reforms were instituted beginning in 1978, the Chinese economy was strictly controlled by the PRC and all business enterprises were owned by the state. Changes in both China's economy and legal system began in 1978, following the death of Mao Zedong in 1976. However, China did not begin adopting modern intellectual property laws until the 1990s.

10.45 It is also important to understand that China has undergone tremendous economic development and cultural changes in the recent past. As one commentator noted, '[i]n the span of just three decades, the People's Republic of

33 Daniel C.K. Chow and Anna M. Han, *Doing Business in China: Problems, Cases, and Materials* (2012), p. 3.

China has managed to lift itself out of poverty and transform itself from an underdeveloped agrarian society to a global economic power'.[34] Thus, as a practical matter, although (as is explained below) China has trade secret laws on the books, it is naive to assume that concepts of unfair competition and business ethics regarding trade secrets are well established in China, particularly since it took the United Kingdom and the United States many decades to fully develop and apply their trade secret principles. Also, the influences of communist ideology, Chinese legalism and Confucianism must be considered to determine how Chinese businesses are likely to view the scope and nature of any obligations of confidentiality.

10.46 Today, China is ostensibly a civil law country that is governed by the 1982 Constitution and statutory law. However, its legal system also reflects the influence of socialist principles. In this regard, the Constitution is not a basis for litigation to exercise rights; it is the basis for exercise of power of the Chinese Communist Party. This does not mean that written law is not applied and enforced, but rather that it is likely to be amended if it does not meet goals established by the Communist Party.

10.47 Under the 1982 Constitution, the National People's Congress (NPC) is the highest legislative body in China, but it is not the only legislative body. There are also legislative bodies at the township, county and provincial levels. However, the influence of these legislative bodies is overshadowed by the Communist Party, led by the President and the Politburo Standing Committee of the Communist Party. As explained by one commentator, '[t]he power structure is really the opposite of its appearance, with a small elite at the top of the structure controlling the broader, less professional constituencies below'.[35]

10.48 Legislative power in China is limited to the NPC and the Standing Committee of the NPC, with both entities empowered to adopt laws of general applicability. The State Council is also empowered to enact administrative rules and regulations on a national level. However, Congresses and people's governments at the provincial level may enact local rules and regulations that apply in their respective administrative regions. These local rules and regulations should not conflict with national laws, but it sometimes does happen and conflicting local provisions must be explicitly repealed.

10.49 In contrast to the legal systems of most common law countries and many civil law systems, China's judicial system is not comprised of three tiers of courts, but

34 *Ibid.*
35 *Ibid.*

instead is a four-tiered system with a number of different 'people's courts'. The Supreme People's Court is the highest court in China with jurisdiction over criminal, civil and economic matters. However, there are also lower Basic People's Courts and a number of other intermediate courts, including the Intermediate People's Court, the Higher People's Court and special military, railway and maritime courts. Within each of China's 26 provinces, a three-tiered system of basic, intermediate and high courts exists, but cases may not proceed through the various tiers due to a 'two trial' rule pursuant to which litigants are only entitled to two hearings on the issues presented in their case. The first involves the initial fact finding and application of applicable law and the second is in the nature of a re-hearing of the evidence.

10.50 Ultimately, the courts must answer to the various people's Congresses, as there is no separation of powers in China and judges do not receive lifetime tenure. Also, if a case is tried in the first instance before the Supreme People's Court, any decision is final.

10.51 Because China is primarily a civil law country, there is no common law jurisprudence and the common law doctrine of *stare decisis* does not apply in China. Decisions by the various People's Courts do not have precedential effect. There is also no systematic reporting of court decisions. Instead, sometimes model cases will be selected by the Chinese judiciary for publication and these cases are meant to educate judges, practitioners, law students and members of the public about how the law should be interpreted and applied. Also, there is a system of legal interpretation that consists of three types with a recognized hierarchy.[36] First, there are legislative interpretations by the applicable legislative bodies which are given the most weight. Second are administrative interpretations by the various governmental units charged with administering the laws. The third type are judicial interpretations (or pronouncements) issued from time to time by the Supreme People's Court.

10.52 Consistent with the legal and economic reforms that began in 1978, China began to accede to the various international agreements concerning IPRs, beginning with the Paris Convention on 19 December 1984 (effective March 1985) and followed by the Berne Convention on 10 July 1992 (effective October 1992). China became a member of the WTO on 11 December 2001, and thus its obligation to comply with Article 39 of the TRIPS Agreement began fairly recently.

36 See Le Wie, 'Judicial Interpretation in China' (1997) 5 *Willamette J Int'l L and Dis. Res.* 87 (1997).

B. Contours of trade secret protection

10.53 Because of the foregoing history, trade secret law in China is in a relatively early stage of development. Trade secrets were first protected in 1993 when the Law of the People's Republic of China against Unfair Competition was enacted. Provisions of this law were later clarified and supplemented in 1998 when the State Administration for Industry and Commerce (SAIC) put into place Several Regulations concerning Prohibition of Acts of Infringement of Trade Secrets. The SAIC is the Chinese governmental body responsible for implementing the trade secret provisions of the Unfair Competition Law (UCL).

10.54 On 12 January 2007, the Supreme People's Court put into effect the Supreme People's Court Judicial Interpretation regarding Various Issues in the Adjudication of Unfair Competition Civil Cases ('Unfair Competition Judicial Interpretation'). Additionally, certain provinces and municipalities have adopted local implementing regulations of the UCL[37] and trade secrets may also be protected under contract law, labour law and intellectual property laws.

10.55 On paper then, trade secret law in China is based upon a robust combination of laws, including the UCL, the Trade Secrets Regulations and the Unfair Competition Judicial Interpretation, together with applicable administrative, judicial and criminal procedures, as described below. However, while Chinese law appears to contain civil, criminal and administrative protections for trade secrets, in practice, they are not very effective. This is one reason why China is often listed on the 'Priority Watch List' of the United States Trade Representative's annual *Special 301 Report*. The *2014 Special 301 Report* explained:

> In particular, the theft of trade secrets remains a significant concern. Such thefts are occurring not only inside but also outside China for the competitive advantage of Chinese state-owned and private companies. Conditions are likely to deteriorate as long as those committing such thefts, and those benefitting, continue to operate with relative impunity, often taking advantage of the theft in order to enter into unfair competition or disadvantageous business relationships with their victims.

10.56 Chinese law recognizes that a broad range of information can be a trade secret, including valuable technical or commercial information that meets the three requirements for protection under article 10 of the UCL. For instance, trade secrets can include such information as manufacturing processes, management know-how, designs, customer lists, marketing strategies and formulas. It also recognizes that information does not need to be in tangible form to be

37 See e.g., Guangdong Province, Hainan Province, Sichuan Province, Henan Province, Shenzhen Municipality and Shanghai Municipality.

protected. Under article 10 of the UCL, a trade secret is 'technical information and business information which (1) is non-public, (2) can bring economic benefits to the party that has rights therein and (3) is practical, and for which the party that has rights therein has adopted measures to maintain its confidentiality'. This is also the language used in the Trade Secret Regulations (article 2)[38] and is consistent with the language of the Uniform Trade Secrets Act (UTSA) and Article 39.2 of the TRIPS Agreement.

10.57 'Non-public' means that the information 'cannot be directly obtained through public channels'. It must have achieved some level of novelty and secrecy. According to the Unfair Competition Judicial Interpretation, information will be considered public and thus cannot be a trade secret if: (1) it is common knowledge or industrial practice for the personnel in the relevant technical or economic field; (2) it only involves a simple combination of dimensions, structures, materials and parts of products, and can be directly obtained through the observation of products by the relevant public after the products enter into the market; (3) it has been publicly disclosed on any publication or any other mass medium; (4) it has been publicized through reporting, exhibition or other channels; (5) it can be obtained through other public channels; or (6) it can be easily obtained without any price. Information that becomes public loses its trade secret protection.

10.58 The economic benefit requirement under the Trade Secrets Regulations, article 2, means that the 'information has a definite applicability and can bring actual or potential economic benefits or competitive advantages to the party that has rights therein'. Abstract ideas and general principles would not qualify as trade secrets without a definite application. Whether information has definite applicability is determined in the context of the industry. Economic benefit is measured by profits (either actual or expected to be generated) from the trade secret, and any lead-time which the owner of the trade secret receives from using it commercially. Thus, actual or potential economic value is required.

10.59 Finally, efforts to protect the confidentiality of the trade secret information pursuant to article 2 of the Trade Secrets Regulations can include the use of confidentiality agreements and confidentiality systems and the adoption of other reasonable confidentiality measures. Similar to the United States, it is a relative standard of maintaining confidentiality and sufficiency will depend on the particular circumstances. Additionally, as in the United States, a contractual statement that information is a trade secret is not binding: as a separate legal determination of the trade secret status of the information must be made.

38 Unfair Competition Law of the People's Republic of China, art. 10.

10.60 The Unfair Competition Judicial Interpretation provides that courts should consider the reasonableness of confidentiality measures based on the nature of the medium containing the relevant information, the intention of the owner to maintain confidentiality, the degree to which relevant confidentiality measures can be identified and the level of difficulty by which others may obtain the information through legal means. If under normal circumstances these factors show that they were sufficient to prevent disclosure of the information, then the measures will be deemed sufficiently appropriate.

10.61 As in the United States, it is permissible to have one trade secret belonging to multiple owners as long as it was developed from independent effort or by reverse engineering. Chinese law prohibits obtaining trade secrets by improper means or by breaching a confidentiality agreement and then divulging or using the trade secret obtained by improper means. Article 10 of the UCL does not consider obtaining information in good faith as improper means, however. Additionally, once a trade secret is disclosed it loses its protection.

10.62 The rights of a trade secret owner are infringed when a person: (1) obtains business secrets by stealing, resorting to coercion or other illegitimate means to acquire the information; (2) discloses, uses or allows others to use the business secrets belonging to another; or (3) discloses, uses or allows others to use the secrets that were obtained by breaking or disregarding the steps taken by the owner to protect the secrets. Misappropriation therefore includes: acquiring the trade secret by illegal or tortious acts; inducement of breach of duty; and disclosing, using or allowing others to use a trade secret obtained by illegal or improper means.

10.63 While 'improper means' is not specifically defined in the UCL, it appears to capture a wide range of conduct, just as in the United States. In one case, for instance, a party who intercepted phone calls to obtain customer information and then used that information to steal customers was found to have misappropriated the information.[39]

C. Trade secrets in employment relationships

10.64 A person who receives a trade secret lawfully but then subsequently uses it unlawfully (like an employee) can be subject to liability for breach of a

39 Zhènjiāng Shì Wúxiàn Shèbèi Gōngsī, Zhènjiāng Shì Dàgōng Kāifā Qū Xīn Hànjiē Shèbèi Chǎng (镇江市无线设备公司, 镇江市大公开发区新焊接设备厂) [*Zhenjiang Municipal Wireless Equipment Co.* v. *Zhenjiang Municipal Dagong Development Zone New Welding Equipment Factory*], Essence of Latest Intellectual Property Decisions and Directions for Handling, 1996 (Zhenjiang AIC, 11 August 1995) (China).

confidentiality agreement in China. The Trade Secrets Regulations (article 3) divides infringement by breach of a confidentiality agreement into two groups: (1) breaches of confidentiality provisions, agreements or restrictions by parties that maintain business relationships with the owner; and (2) breaches of confidentiality provisions, agreements or restrictions by employees of the proprietor or owner.

10.65 The Labour Law of the People's Republic of China, in article 22, permits parties to a labour contract to agree to the protection of trade secrets. Thus, to make certain that employees fall under the second category noted above, it is generally advisable to obtain a written labour contract that contains provisions restricting the use and disclosure of trade secrets both during and after employment. When doing so, however, keep in mind that the provisions of China's Labour Law and Labour Contract Law must be followed carefully. For instance, article 19 of the Labour Law requires that such agreements be written in Chinese and that they include clauses related to the term of the contract, working conditions, discipline and conditions for termination of the contract. Article 17 of the Labour Contract Law has similar requirements and also requires that terms regarding social insurance, working hours and job specifications be included in the contract.

10.66 While a contractual agreement with employees is always recommended, in theory, it is not necessarily required for an employer to state a claim for breach of confidentiality in China. It may be enough that the owner or employer communicated to the employee its requirement to keep the information confidential. This would cover those employees who are not bound by a labour contract. As to higher level employees, article 149 of the Company Law in China prohibits directors, supervisors and managers of a limited liability company or a joint stock limited liability company from divulging secrets of the company.[40]

10.67 Article 102 of the Labour Law provides that if an employee breaches the confidentiality provisions of a labour contract, he will be liable to compensate the employer. However, it does not provide a method for determining the damages to be paid to the employer. Under article 20 of the UCL, the infringer of a trade secret should pay damages in an amount that equals the actual losses suffered by the owner, or if the losses suffered by the owner are difficult to ascertain, the amount which equals the profits earned by the infringer. Thus, if an employer hires an employee who has not terminated his labour contract with

40 Company Law of the People's Republic of China (promulgated by the National People's Congress, 27 October 2005, effective 1 January 2006) 2006 China Law LEXIS 7956 (China).

a former employer and obtains trade secrets of the former employer from the new employee, the new employer is responsible for compensating the losses suffered by the former employer.[41]

10.68 Ownership rights with respect to technology have been clarified under the new Contract Law of China, article 326. It provides that technology developed by an employee while performing the tasks to which he has been assigned by his employer and while using his employer's materials and resources belongs to the employer. However, similar to the law of Japan (discussed below), the employer must compensate the employee for the use and/or transfer of the technology and the employee has the right of first refusal with respect to any assignment or licensing of the technology.[42] This could be problematic for foreign companies which have required employees to assign all rights to any inventions developed on the job, particularly if they have not provided additional compensation for the use of the inventions. They may also be restricted by the requirement that the employee has the right of first refusal with respect to assignments or licensing of the technology developed by the employee.

10.69 Generally, employers and employees may enter into non-compete agreements in China, but the Labour Contract Law specifies that the employee must be compensated for the period of post-termination non-competition. The Labour Contract Law also states that non-compete agreements apply only to senior management, senior technical personnel and other employees with confidentiality obligations. The parties are to agree on the scope, territory and period for these non-compete obligations. However, in no case may the period of non-competition exceed two years.

10.70 Due to a lack of clarity concerning the required compensation for non-compete agreements, the Supreme People's Court released Judicial Interpretation IV on Several Issues concerning the Application of Law in Hearing Labour Dispute Cases ('Judicial Interpretation IV') that went into effect on 1 February 2013. This and any later pronouncements should be consulted when drafting non-compete agreements and any other labour contract for use in China, but generally, Judicial Interpretation IV confirms that former employees must be paid for the period of non-competition and specifies that the courts will award 30 per cent of the employee's previous annual salary. It also details how non-compete agreements may be terminated by employers and employees.

41 Unfair Competition Law of the People's Republic of China, art. 20.

42 Contract Law of the People's Republic of China, art. 326 (promulgated by Order No. 15 of the President of the People's Republic of China on 15 March 1999).

10.71 As discussed in Chapter 5, when implementing a trade secret protection strategy, it is never advisable to rely upon an implied duty of confidentiality, whether in China or elsewhere. Because it is difficult to successfully pursue trade secret claims in China, it is recommended that companies enter into signed agreements with their employees to protect trade secrets, acquire signed acknowledgments of receipt of trade secrets and conduct exit interviews where employees sign acknowledgments that they have received trade secrets. Keep in mind, however, that ancillary areas of law, such as competition laws or special laws governing employment relationships, may restrict the scope, nature and enforceability of such agreements.

D. Trade secrets in business relationships

10.72 Doing business in China, like all other countries, not only requires an understanding of the laws that govern business relationships, but the traditions and culture of China. Particular consideration must be given to how products are manufactured in China and the various companies that can be involved in the process, from the beginning of the supply chain to the end. As one commentator noted:

> While the foreign customer may be able to require its China sourcing agent or vendor to execute an appropriate confidentiality agreement, it can be extremely difficult to ensure that all vendors, employees, suppliers, sub-vendors, sub-contractors, and all of their employees also sign appropriate agreements, or abide by the measures to maintain the confidentiality of Trade Secrets. In fact one of the reasons that China is a good source of low cost manufacturing is the flexibility of its supply chains.[43]

10.73 It is also important to consider the contracting practices of Chinese businesses. In this regard, not unlike Japan and other Asian countries, a commentator has noted:

> China is a high context society, that is, a society in which most people share a common set of norms, values, and beliefs that create a starting point for any business negotiations. When Chinese parties negotiate among themselves, a great deal can be left unsaid and communications are often indirect because of this shared context.[44]

Where US lawyers and their clients may prefer detailed and precise (almost harsh) legal agreements, Chinese business people are likely to prefer more relaxed and polite language, with the context of the business relationship

43 Laura Wen-yu Young, 'Protecting Trade Secrets in China' in *Trade Secrets 2013: What Every IP Attorney Should Know* (2013), p. 242.

44 Chow and Han, n. 33 above, p. 63.

defining many of the legal obligations. Thus, it is important to know the customary obligations of various relationships, which are often based upon principles of Confucianism and respect for hierarchy.

10.74 As in Brazil and India, there are specific laws in China that concern technology transfer.[45] China's Contract Law, Part 18, deals with technology contracts, including those involving the development and transfer of trade secrets and know-how. Article 43 addresses the protection of trade secrets that are revealed during contract negotiations:

> trade secrets learned by a party during the course of concluding a contract may not be disclosed or improperly used, regardless of whether the contract is concluded or not. If a party causes loss to the other party through the disclosure or improper use of such trade secrets, he is liable for damages.

10.75 Similar to the law of the United States, client or customer lists are protectable as a trade secret in China; however, a mere listing of names is not sufficient. Additional information including contact information, client preferences and price tolerance or preferences must also be included. Also, the additional information should be different from the kind of list that would be obtained from public channels. Further, the list must be confidential and the subject of reasonable measures taken to prevent others from obtaining it. A Chinese court may also take into account the difficulty, expense and staffing involved in creating the list.

E. Criminal consequences for trade secret misappropriation

10.76 Article 219 of the Criminal Law of the People's Republic of China makes it a crime of trade secret misappropriation to: (1) obtain trade secrets of another party by theft, enticement or other unfair methods; (2) divulge, use or allow others to use another party's trade secrets; or (3) divulge, use or allow others to use trade secrets in breach of an agreement or contrary to a confidentiality agreement. The definition of trade secrets within the scope of punishable activity is similar to that provided under the UCL. However, it can be difficult to convince the authorities to file criminal prosecutions and perceived high profile cases are more likely to receive attention.

---

45 For more on general contract law in China in the context of international business transactions, see Nicole Kornet, 'Contracting in China: Comparative Observations on Freedom of Contract, Contract Formation, Battle of Forms and Standard Form Contracts' (2010) 14.1 *Electronic Journal of Comparative Law* (May), available at www.ejcl.org/141/abs141–1.html.

10.77 Generally, to be held responsible for criminal trade secret misappropriation in China, a defendant must have intent, but when he or she receives trade secrets that are wrongly disclosed, his knowledge that the information was a trade secret might be enough. To be a crime under article 219, however, the conduct must cause 'serious losses' or 'extremely serious consequences' to the owner.

10.78 The maximum penalty for 'serious losses' is imprisonment for three years and/or a fine. For 'extremely serious consequences' the penalty is increased to imprisonment of not less than three years, but no more than seven years and a fine. Where the offender is an organization, the organization will be subject to a fine. The management personnel in charge of the organization and the person directly responsible for the criminal act will be subject to the penalties of imprisonment and/or a fine.

10.79 In May 2011, the Supreme People's Procuratorate and the Ministry of Public Security issued new regulations for trade secret misappropriation specifying that criminal prosecution should be instituted: (1) where a trade secret owner suffers losses of more than RMB500,000; (2) becomes bankrupt from the infringement; (3) suffers grave losses; or (4) the amount of the legal gains from the infringement is more than RMB500,000. Depending upon the applicable exchange rate, the RMB500,000 figure equals approximately US$80,000.

10.80 Under the UCL and the Trade Secrets Regulations, administrative sanctions that are quasi-criminal in nature are also available for trade secret misappropriation. These can be imposed by administrative agencies directly without going through the courts.

10.81 The UCL protects both the owner of the trade secret and its licensees from trade secret misappropriation. Since there is no registration of trade secrets, the owner of a trade secret must prove to the enforcement agencies that the trade secret exists and that it owns or has the right to use the trade secret. Note that administrative sanctions are not available to a party who obtains, discloses or uses the trade secret if he does not have a profit motive. The requirement of a profit motive in article 10 of the UCL means that use of the trade secret for any non-profit activity, such as scientific research, does not violate the law.

F. Litigating trade secret disputes

10.82 Enforcement of trade secret misappropriation in China can be very difficult due to the nature of the legal system and the fact that administrative enforcement authorities (the Administration for Industry and Commerce (AIC)) tend to be

conservative in their approach to these cases and often encourage parties to use the courts instead.

10.83 Article 20 of the UCL provides civil liability for misappropriation of trade secrets. The operator of a business who commits trade secret misappropriation is liable for damages and reasonable costs incurred by the owner of the trade secret to investigate the alleged acts of misappropriation by the defendant. In addition to damages, the court may also require that the misappropriator accept civil liability under the Civil Code. This may include stopping ongoing acts of misappropriation, eliminating the adverse effects of the misappropriation by requiring the defendant to keep the trade secret confidential and not divulge it, returning the trade secrets and offering an apology (which may need to be approved by the court before it is published in the newspapers).

10.84 The trial level courts for trade secret infringement cases are usually the Intermediate People's Court. Other courts may be designated to accept trade secret cases, including local courts that have already been approved to hear civil cases involving intellectual property rights.

10.85 Pursuant to the Unfair Competition Judicial Interpretation a party claiming that someone else has misappropriated its trade secret has the burden of proving: (1) that its information meets the statutory requirements of a trade secret; (2) that the alleged infringer's information is similar or substantially similar to its trade secret; and (3) that the alleged infringer has used unfair means. An exclusive licensee may also commence a misappropriation action on its own (or jointly with the owner) and a non-exclusive licensee may commence an action jointly with the owner or on its own, provided that it has the written authorization of the owner.

10.86 The Judicial Interpretation also provides that when the court issues an injunction against infringement of a trade secret, the length of the injunction should generally be extended to the time when the trade secret becomes known to the general public. The amount of damages for trade secret misappropriation may be determined by considering actual loss caused to the owner and the benefit received by the infringer. Where the infringement causes the trade secret to be revealed to the general public, the damages will be determined according to the commercial value of the trade secret. Commercial value includes such considerations as the research and development costs, the proceeds from using the trade secret and the time for maintaining the competitive advantage resulting from the trade secret.

10.87 Consistent with the language of footnote 10 of the TRIPS Agreement, third parties are liable for trade secret misappropriation in China only if they know or should have known that a trade secret was obtained by improper means or in breach of a confidentiality agreement.[46] Thus, a third party should exercise diligence to ascertain that any information it receives is not trade secret information obtained in that manner. If, however, the third party is put on notice that the trade secret was obtained improperly and chooses not to learn additional facts, he or she may not be protected. If a third party acts in good faith and without knowledge of the improper means, it will not be liable for divulging or using the trade secret.

10.88 Evidence of trade secret misappropriation can be difficult to obtain in China because discovery is limited. There are a number of investigative firms that conduct such investigations and some may require government approval. Some courts may refuse to admit evidence collected outside of legitimate channels. Also, evidence for the court proceedings should generally be notarized. This might require involving the PRC Notary Public in the process of collecting the evidence. Not much weight is given to affidavits and witness testimony, but greater weight is given to physical evidence and documentary evidence. Although the courts have the power to help parties gather evidence, this power is not often used.

10.89 Article 135 of the Civil Code of China provides that the limitation period for bringing a civil action is two years unless provided otherwise. The limitation period starts to run from the date when the plaintiff knew or should have known of the infringing act.

10.90 Because the plaintiff in a misappropriation case has to show that the trade secret exists, there is a risk of disclosing additional trade secrets to the defendant. Article 68 of the Civil Procedure Law provides that the trade secret should be kept confidential during litigation and that evidence relating to the trade secret should not be produced in open court. In general, Chinese courts usually hear trade secret cases *in camera.* However, *in camera* review is not as comprehensive as it is in the United States and information is still accessible to litigants and their agents. Only the general public and mass media are excluded.

10.91 Generally, preliminary injunctions are very rare and difficult to obtain in China and will not be granted before the commencement of an action. Also, as it currently stands, the People's Court does not have the power to grant preliminary injunctions to prohibit a misappropriator from using or divulging a trade

46 Unfair Competition Law, art. 10.

secret. In deciding whether to grant preliminary relief, Chinese courts will consider whether the relationship of rights and obligations between the parties is definite and if the denial of the preliminary order would seriously affect the life or business of the applicant.[47] Permanent injunctions are more likely because they are granted after a plaintiff has proven its case.

10.92 Recent revisions to the Civil Procedure Law have introduced 'conduct preservation' orders pursuant to article 100. This allows a party to request that the court issue an order to freeze the assets of another party or require another party to perform or not perform certain acts prior to trial. These may prove quite useful in trade secret cases. This procedure may be used indirectly (as a kind of preliminary injunction) to prevent the infringer from divulging, using or permitting others to use the trade secrets of the plaintiff.

10.93 Evidence preservation orders are available and have become relatively routine in trade secret cases pursuant to article 81 and article 101 of the revised Civil Procedure Law. These appear similar to Anton Piller orders under UK law, discussed in Chapter 9, and can be issued *ex parte*. Since there is no pretrial discovery available to plaintiffs in China, this procedure may be utilized to preserve and obtain documents. Preservation orders may be granted if it is shown that without preservation the complainant will suffer irreparable damage. If granted, the applicant is required to provide a guarantee (a bond or security) to the court to compensate for the losses to the respondent if the order should not have been granted. According to article 101, the applicant must commence legal proceedings within 30 days of the order, and if it fails to do so, the preservation order will automatically be rescinded.

10.94 As in common law jurisdictions, the general rule in China is that a party asserting an allegation of trade secret misappropriation bears the burden of proof. However, because China does not have a pretrial discovery system, the plaintiff in a trade secret misappropriation case must use other means to collect sufficient evidence to meet its burden. Generally, evidentiary requirements in civil lawsuits are stricter than those in administrative proceedings. In some circumstances a court may itself collect evidence because courts in China have the right to obtain evidence from relevant entities and individuals, and parties may request that the court collect evidence that is not obtainable by the parties.

10.95 In light of the discovery and evidentiary difficulties of civil cases in China, the better approach may be for trade secret owners to combine administrative and

47 Civil Procedure Law, art. 107 (adopted at the 28th Session of the Standing Committee of the 11th National People's Congress on 31 August 2012).

judicial enforcement. This could mean filing an administrative complaint with the AIC for determination of infringement and an injunction and then filing a separate court action for compensation. One advantage to this approach is that information obtained from an administrative raid may help with deciding whether subsequent judicial action or civil litigation is advisable. A decision by the administrative authority may also be used to support the court action.

10.96 Another alternative, particularly with respect to business-to-business relationships, is for the parties to arbitrate their dispute, provided that there is an enforceable written arbitration agreement between the parties. Arbitration has become the preferred method for resolving business disputes in China, with the China International Economic and Trade Arbitration Commission (CIETAC) and similar arbitral bodies being established for such purpose. However, the availability of preliminary relief is typically more limited in arbitral settings and, depending upon the arbitral forum selected, often it cannot be imposed without the agreement of the parties and cannot be enforced without court intervention.[48]

10.97 While the Trade Secrets Regulations and UCL is interpreted by the SAIC's Fair Trade Bureau, enforcement is actually carried out by the AIC, a body of the various local governments. The AIC generally acts in response to complaints filed by trade secret owners. If direct negotiations with an alleged misappropriator have not been successful, the trade secret owner may file a complaint with the AIC at or above the county level or start a court action. Article 5 of the Trade Secrets Regulations requires that the complainant provide evidence of the existence of the trade secret and of the infringing act. If the proprietor cannot produce evidence to prove that the alleged misappropriator obtained the information improperly, it may still file a complaint with the AIC.

10.98 Applicable law further provides that:

> [T]he Authority for Administration of Industry and Commerce may determine on the basis of the relevant evidence that the respondent has committed a misappropriation infringement if (i) the party that has rights in the trade secrets can prove that the information used by the respondent is consistent or identical with its own trade secrets and, in addition, that conditions existed under which the respondent could obtain the trade secrets; and (ii) the respondent is unable or refuses to provide evidence that the information used was lawfully obtained or used.

48 See CIETAC Revised Rules, arts 21.1 and 21.2.

This provision shifts the burden of proof from an owner of the trade secret to the respondent after the owner proves that the respondent is: (1) using the trade secret; and (2) could have obtained a trade secret from the owner. The respondent must rebut this presumption of misappropriation by showing that it obtained or used the information lawfully. If the alleged infringer is unable to do so, the AIC may find him liable for misappropriation of the trade secret. Throughout this process, AIC officials are required to keep the trade secrets of the complainant confidential. This means that they should not disclose trade secrets to the respondent while handling the case.

10.99 Where the complainant shows that the respondent's use or disclosure of the trade secret to others would cause irreparable losses to the complainant, and upon the provision of a written guarantee to AIC to assume potential liability for compensating the losses which may be suffered by the respondent, AIC may seize the drawings, software and other documents containing trade secrets that were obtained by the respondent through improper means. It can also order that the respondent stop selling products manufactured with the trade secrets, pending additional investigation by the AIC. The AIC may also order the respondent to return documents containing the trade secrets and supervise destruction of goods manufactured with the trade secret unless the owner agrees to other methods of disposal of these goods. However, the AIC does not have the power to order the respondent to provide compensation to the trade secret owner.

10.100 If the respondent refuses to follow the punishment decision of the AIC and continues to infringe, the new acts of infringement may be punished separately. If the respondent objects to the punishment decision made by the AIC, it may apply to the AIC at the next higher level for administrative reconsideration or it may take the matter to court for a ruling. The AIC also has power to mediate the question of damages or the trade secret owner may seek damages in court.

IV. JAPAN

A. Overview of the legal system

10.101 Japan has a rich legal history.[49] As described by one commentator, '[t]he Japanese legal system represents an amalgam of at least three distinct legal

49 See generally Hiroshi Oda, 'The History of Japanese Law' in *Japanese Law* (1992), pp. 14–32, reprinted in Kenneth L. Port, *Comparative Law: Law and the Legal Process in Japan* (2nd edn 2003), pp. 20–33.

orders patched together during two major junctures in the Nation's history'.[50] Initially, it was a feudal system but in the late 1800s, under pressure from Western influences, it migrated to a civil law system by adopting a Constitution based upon the Constitution of Prussia (the Constitution of the Empire of Japan 1889, or the 'Meiji Constitution') and laws based upon the codes of Prussia, Germany and France. It was also an early member (since 1889) of both the Paris Convention and the Berne Convention, thereby agreeing to protect the IPRs described therein.

10.102 After the Second World War, under pressure from the United States and its allies, Japan began to adopt many legal principles of American law, including a revised Constitution based upon requirements of the Potsdam Declaration, a governmental structure that features three independent branches and an anti-monopoly law that is similar to US law.

10.103 Today, the legal system in Japan is similar in many respects to the legal system of the United States with a three-tiered judicial system, a Constitution that is the supreme law of the land and a variety of sources of law.[51] But there are important differences that can frustrate those who are used to US-style procedure and litigation. Of particular importance is the way that the Japanese think about the law and the fact that there is more about Japanese law and legal practice than can be found in written codes or guidelines. As one commentator explained:

> Westerners who seek to enter the way of law in Japan often are frustrated by what appears to be a house of mirrors. Texts that seem to speak clearly and directly are routinely evaded. On the other hand, when the law is silent, behavior still conforms (or is expected to conform) to the accepted norm.[52]

The key in Japan is to understand the Japanese conception of law and to work within it, understanding that '[t]he words are merely signposts'.[53]

10.104 With respect to matters of civil procedure, there are significant differences between the judicial systems of Japan and the United States (although some changes have been made in recent years with respect to IPR enforcement, as

50 Donald L. Uchtmann, Richard P. Blessen and Vince Maloney, 'The Developing Japanese Legal System: Growth and Change in the Modern Era' (1987/88) 23 *Gonz. L Rev.* 349.

51 Francia Evers, 'Sources of Law', reprinted in Port, n. 49 above, pp. 43–52. See also Japan Federation of Bar Associations, www.nichibenren.or.jp/en/; Supreme Court of Japan, www.courts.go.jp/english/; Nihonkoku Kenpo (Japanese Constitution), arts 76–82 (Japan).

52 Dan Rosen, 'The Koan of Law in Japan' (1990) 18 *N Ky L Rev.* 367, reprinted in Port, n. 49 above, p. 35.

53 *Ibid*. 36.

discussed below).[54] First, the availability and scope of pretrial discovery is limited. Second, there are no jury trials in Japan and the cost to initiate litigation is generally higher than in the United States. Third, Japanese courts do not have the power to enforce injunctive relief through contempt proceedings. Also, due to the legal history of Japan and its culture, the Japanese people tend to hold anti-litigious sentiments depending upon the nature of the dispute. Thus, the Japanese legal system often places greater emphasis on private and customary methods of dispute resolution than does the US system.

10.105 As defined by the Japanese Constitution, the judicial system in Japan consists of the following courts: the Supreme Court; the High Courts; the District Courts; the Family Courts; and the Summary Courts.[55] The last three courts are all courts of first impression, with Summary Courts being reserved for disputes of low monetary value. In 2005, in response to US criticism that the resolution of patent cases was too slow, Japan created a special High Court to handle certain intellectual property cases that is similar to the US Federal Circuit Court of Appeals.[56] Because the special Intellectual Property Court does not handle trade secret matters, a claim for trade secret misappropriation in Japan is initiated in a District Court and, if necessary, appealed first to a High Court of the applicable jurisdiction and then to the Supreme Court of Japan.

10.106 Due to its legal history and the many influences on Japanese law, Japan is primarily a civil law country (like Germany and France), but with aspects of a common law country.[57] According to the 1947 Japanese Constitution, the Diet (the Japanese Parliament) is the sole law-maker in Japan and the primary source of law in Japan is the written code adopted by the Diet. However, there are a number of secondary sources of law that must be considered. These include (in order of hierarchy): written laws, cabinet orders, administrative rules, judge-made law, custom, treaties, administrative guides and scholarly opinion. With respect to treaties, because they must be approved by the Diet, they are considered to be self-executing and, therefore, are a direct source of law in Japan.

10.107 The common law aspects of Japanese law are reflected in the role of the judiciary in interpreting and applying the code and the precedential value of

54 Nobutoshi Yamanouchi and Samuel J. Cohen, 'Understanding the Incidence of Litigation in Japan: A Structural Analysis' (1991) 25 *International Lawyer* 443, reprinted in Port, n. 49 above, pp. 102–7.

55 Perry R. Luney, Jr, 'The Judiciary: Its Organization and Status in the Parliamentary System' (1990) 53 *Law and Contemp. Probs* 135, reprinted in part in Port, n. 49 above, pp. 61–9.

56 John Tessensohn and Shusaku Yamamoto, 'Japan: Intellectual Property – Establishment of Japan Intellectual Property High Court' (2005) 27(8) *Eur. Intell. Prop. Rev.* N161.

57 Port, n. 49 above, at 9.

court decisions, particularly those of the Japanese Supreme Court. The decisions of the Supreme Court are precedent with respect to lower courts and can be used to fill gaps which exist in the codes.[58] However, Japanese courts are not as bound by precedent as US courts. Thus, sometimes the Supreme Court of Japan will not follow its own precedent and lower courts will not follow earlier decisions of the Supreme Court. Despite the foregoing, the decisions of Japanese courts can and should be analyzed to determine how Japanese trade secret principles have been applied in practice.

10.108 The Japanese government takes much more of an active role in the management of the Japanese economy than does the government of the United States and many other countries. As a result, an important secondary source for an understanding of Japanese law is the various pronouncements and guidelines issued by governmental agencies. As one commentator explained, '[a]dministrative guidance is an informal instrument used by administrators that is usually addressed to private corporations'.[59] In the case of IPRs, the important administrative guidelines are typically issued by the Ministry of Economy, Trade and Industry (METI) (which includes the Japan Patent Office (JPO)).

10.109 Like the federal law of the United States, the law of Japan is national in scope.[60] The laws that relate to the scope and enforcement of trade secret rights include the Unfair Competition Prevention Law (discussed below), the Civil Code, the Code of Civil Procedure and the Antimonopoly Act. The codes and standards concerning labour and employment must also be considered with respect to the various employee agreements discussed in Chapter 4.

B. Contours of trade secret protection

10.110 Historically, Japan was not aggressive in the protection of IPRs, including trade secrets, owing in part to cultural beliefs that exalt the good of the community over the good of the individual.[61] In this regard, although Japan adopted many parts of the German code in the 1930s, it did not adopt the trade secret provisions of that code.[62] Until the early 1990s, trade secrets were protected in Japan, if at all, pursuant to a variety of tort and contract theories.[63] Consistent

58 Evers, n. 51 above. See also Supreme Court of Japan, www.courts.go.jp/english/.

59 Evers, n. 51 above, at 51.

60 Chiho jichi ho [Local Autonomy Act], Law No. 67 of 1947 (Japan).

61 Pantea M. Garroussi, 'Technology Transfers to Japan: Legal and Cultural Frameworks' (1997) 26 *Colo. Law* 77.

62 Holly Emrick Svetz, 'Japan's New Trade Secret Law: We Asked for It – Now What Have We Got?' (1992) 26 *Geo. Wash. J Int'l L and Econ.* 413, 420.

63 Jay Dratler, Jr, 'Trade Secrets in the United States and Japan: A Comparison and Prognosis' (1989) 14 *Yale J Int'l L* 68, 99–110 (describing the state of Japanese trade secret law before the amendments to the law that are detailed in this chapter).

with the same problems encountered by the United States until the adoption of the UTSA, the problem with the use of Japanese contract and tort law to protect trade secrets was its limited application. In the case of contract claims, the principal problem was the inability to hold third parties liable for trade secret misappropriation if they were not in privity of contract. With respect to tort claims, the principal problem was the limited view of enforceable 'legal rights' under Japanese law.

10.111 Although Japan has been a long-time member of the Paris Convention and adopted its Unfair Competition Prevention Law (UCPL) in 1934 to comply with the Hague Amendments to the Paris Convention, during the early stages of the negotiations that led to the TRIPS Agreement, Japan was among a group of countries that did not see trade secrets as a form of IPR.[64] Japan's views with respect to trade secrets began to change after the United States adopted the Omnibus Trade and Competitiveness Act of 1988[65] and thereafter exercised the authority granted the US Trade Representative to issue reports concerning IPR protection afforded by various countries. In the first of these reports (and some subsequent reports), Japan was listed as a principal violator of IPRs.

10.112 Soon after the first report by the US Trade Representative, the MITI (a predecessor, in part, to the METI) initiated efforts to draft a trade secret code modeled on the UTSA that was later approved by the Diet. Significantly, this code (part of the aforementioned UCPL) was adopted in 1990, years before the language of Article 39 of the TRIPS Agreement was finalized and, thus, includes a differently worded definition of a trade secret than the TRIPS Agreement. The frequency of subsequent amendments to the UCPL (as explained below) may be attributed to pressure by the United States for Japan to improve its protection of IPRs and the Japanese government's realization of the importance of IPR protection for Japan's own economic development.[66] It is also explained by the civil law system of government that requires frequent re-evaluation and amendments to the written code.

10.113 The initial amendments to the UCPL to include trade secrets were adopted by the Diet on 22 June 1990, pursuant to Law No. 66.[67] Further changes were promulgated in 1993 consistent with efforts by the World Intellectual Property

64 In a submission by Japan to NG11 on 12 September 1988 regarding the desired scope of the TRIPS Agreement, no mention was made of trade secrets. See Submission of Japan, MTN.GNG/NG11/W/17/Add. 1.

65 Pub. L No. 100–418, 102 Stat. 1107 (codified as amended at several sections of 19 USC) (1988).

66 See Tessensohn and Yamamoto, n. 56 above (describing Japan's pro-patent policy since 1997).

67 Kazuko Matsuo, 'Recent Amendment to the Unfair Competition Prevention Law for the Protection of Trade Secrets' (1991) 9 *UCLA Pac. Basin LJ* 78, 79, Appendix. See also Svetz, n. 62 above, at 424–5.

Organization to harmonize unfair competition laws. This new law (Law No. 47) became effective on 1 June 1994.[68] The UCPL was subsequently amended several times, with significant amendments for trade secret purposes being in 2003, 2005 and 2009.[69] As is the practice in civil law countries like Japan, further review of the UCPL is anticipated on a regular basis, including a pending review that is due to be completed in 2015 and which may result in further amendments.

10.114 As a practical matter, the foregoing history means that the development of trade secret jurisprudence in Japan is 25 years old and that fewer case decisions exist to explain the application of the law than in the United States. In fact, between 1991 and 2014 there were only approximately 160 court decisions in Japan in matters involving trade secrets and only one criminal prosecution.

10.115 As it has evolved, the trade secret law of Japan is now very similar to the law of the United States as expressed in the UTSA, but this has been the result of incremental change rather than a full embrace of all US trade secret principles. Initially, even though the trade secret provisions of the UCPL went into effect in 1991, they were not used much by Japanese companies because there was not much actual or perceived trade secret misappropriation by Japanese workers. Also, foreign companies doing business in Japan did not file many trade secret misappropriation cases because they feared the exposure of their trade secrets during litigation, a situation that Japan has sought to resolve in recent years.

10.116 As currently written, the UCPL consists of 26 articles,[70] many of which concern trademark, domain name and false advertising provisions that are similar to section 43 of the Lanham Act of the United States.[71] With respect to trade secrets, the UCPL begins in article 2 by defining unfair competition in language that is similar to the definition of misappropriation under the UTSA. Specifically, article 2(1)(iv) through (ix) includes a litany of wrongful acts that define the wrongful acquisition, disclosure or use of trade secrets in three basic circumstances.[72] The first circumstance concerns how the subject trade secret information was acquired and mirrors the 'improper means' provisions of the UTSA. The second circumstance concerns the wrongful disclosure or use of trade secrets after they have been rightfully (for instance, as part of a licensing or

68 Japan Patent Office, *Outline of the Japanese Competition Prevention Law* (2008), p. 3.

69 *Ibid*. 3–5. (Note: The frequent changes to the UCPL mean that the numbering of the various articles of the UCPL may have changed somewhat over time, requiring the tracing of those changes to understand any commentary and case references which predate the most recent changes.)

70 Fuseikyoso Boshiho [Unfair Competition Prevention Act], Law No. 47 of 1993 as amended by Act No. 62 of 2011 (effective 1 December 2011).

71 15 USC 1125 (2012).

72 Matsuo, n. 67 above, at 203.

manufacturing agreement) or wrongfully acquired. The third circumstance concerns the acquisition, disclosure or use of trade secrets by individuals or companies that were not the direct misappropriators (third parties) and specifies that such individuals must have knowledge of the earlier misappropriation or be 'grossly negligent' in not knowing.

10.117 Article 2(1)(vii) is the provision of the UCPL that concerns the use or disclosure of a trade secret that was acquired rightfully as part of a confidential relationship, although the terminology 'confidential relationship' is not used. Instead, the provision concerns 'a trade secret which has been disclosed by the business entity holding it'.[73] According to this provision, the individual or company that possesses the trade secrets of another will be liable for trade secret misappropriation if they disclose or use the trade secrets 'for the purpose of acquiring illicit gain, or causing injury to the holder'. As with US law, the extent and nature of the duties of the person or entity to which trade secrets are disclosed is defined elsewhere, often pursuant to general principles of unfair competition or contractual obligations.

10.118 With respect to the definition of a trade secret, article 2(6) of the UCPL provides that: the term 'trade secret' means 'technical or business information useful in commercial activities, such as manufacturing or marketing methods, which is kept secret and not publicly known'. Some commentators have indicated that such a definition is broader than the definition of a trade secret under US law because it explicitly recognizes that business (as opposed to technical) information can be a trade secret,[74] but US law has long protected non-technical business information. The real question under the interpretation and application of Japanese law is whether the use of the phrase 'technical or business' serves as a limitation on the scope of protectable information.

10.119 As translated into English, the definition of a trade secret in the UCPL is similar to the multipart definition of a trade secret under both Article 39.2 of the TRIPS Agreement and the UTSA, although the three requirements are expressed differently. Secrecy is defined as 'not publicly known'; commercial value is defined as 'useful in commercial activities'; and reasonable steps is defined as 'kept secret'. The terms 'commercial' or 'economic' value are not used and the 'readily accessible' language is missing.

10.120 On the surface, one might read Japan's definition of a trade secret to be both narrower and broader than the UTSA definition. It seems narrower because the

73 Japan Patent Office, n. 68 above, at 21.

74 Svetz, n. 62 above, at 426.

requirement of 'usefulness in commercial activities' appears to require actual use of the information in the putative trade secret owner's business, a concept that the UTSA intentionally rejected over earlier case law in the United States and that was replaced with the concept of 'independent economic value'. However, at least one Japanese court has applied an expansive view of the usefulness requirement so that the information need only 'be helpful for the trade secret owner to save relevant costs or improve the operation of the business'.[75]

10.121 A commentator who was involved in drafting the trade secret provisions of the UCPL confirms an expansive definition of a trade secret under Japanese law, explaining that 'almost any information may be claimed as a trade secret, as long as it falls within the scope of technical or business information, and it will probably be easy to say that it falls within that scope'.[76] However, he also notes that the requirement of 'being useful in commercial activity' was intended to limit the scope of protectable trade secrets by excluding information 'which is not worth protecting under the legal system because of a lack of social necessity, social benefit, or justice'. This includes scandalous information, information concerning tax evasion and information regarding non-compliance with environmental laws, but would not include negative information concerning failed research and development.

10.122 The definition of a trade secret under the UCPL is arguably broader than under both the UTSA and Article 39 of the TRIPS Agreement because, on the surface, the definition of applicable prior art is limited to what is 'publicly known'. Not included in the explicit language of the UCPL is the recognition that 'publicly known' can include information that is well known within a given industry, even if it is not known by the general public. Also, there is no explicit mention of information that is 'readily accessible' or 'readily ascertainable'. However, METI guidelines and some court decisions suggest a broader definition of trade secret disqualifying prior art to include both information that is well known within a given industry or trade and information that is readily ascertainable.[77] Also, a commentator noted in 1991 that the opinions in patent cases will probably be applied to define prior knowledge.[78] In this regard, the

75 Hyun-Soo Kim, *Trade Secret Law, Intellectual Property and Innovation: Theoretical, Empirical and Asian Perspectives* (unpublished Ph.D dissertation, University of Illinois at Urbana-Champaign, 2010), p. 81, available at http://hdl.handle.net/2142/18387, citing Tokyo District Court of Japan, 14 February 2002, Heisei 12 (Wa) 9499 (Japan).

76 Matsuo, n. 67 above, at 82.

77 Kim, n. 75 above, at 83.

78 Matsuo, n. 67 above, at 83.

Japan Patent Office has stated that the not publicly known refers 'to a state where [the information] cannot generally be obtained, except under the holder's control'.[79]

10.123 Similar to the US requirement of 'reasonable efforts to maintain secrecy', the UCPL requires that to qualify for protection as a trade secret, information must be 'kept secret'. In practice in Japan, this is the most important requirement of the definition of a trade secret and the factor that garners most of the attention of courts and commentators. However, like the UTSA, the UCPL does not explicitly define what measures are needed to keep something secret, leaving it up to the courts to determine what is adequate under the particular circumstances of each case. However, it is generally believed that Japanese law is more stringent in defining the required secrecy efforts than is true under US law. A person who was involved in drafting the requirement explained:

> It is clear that the means of administration used will vary according to the importance of the trade secret and size of the enterprise, according to whether it is a tangible or intangible trade secret, according to whether a trade secret is in an early stage or closer to the stage of completion, and according to other various characteristics, situations, or circumstances.[80]

10.124 The foregoing is similar to trade secret law as it is applied in the United States. What is different is the explicit understanding that was reached during the UCPL drafting process that something more than a subjective desire to keep information secret is required. Similar to the case decisions of several US states and the notice purpose of the reasonable efforts requirement of US law,[81] Japan requires that objective efforts to maintain secrecy must be shown in order to give 'clear notice of the secret nature of the information to persons who have access to the trade secret'.[82] According to METI guidelines issued in 2003, two basic requirements must be met. First, only designated individuals can have access to the information. Second, the recipient of the information must be able to recognize that the information is a trade secret.[83]

10.125 Further guidance issued by METI sets forth a litany of efforts or 'desired standards' that should be considered by businesses to determine whether information has been administered in secret.[84] These are organized around a

---

79 Japan Patent Office, n. 68 above, at 20.

80 Matsuo, n. 67 above, at 83.

81 See Chapter 3.

82 Matsuo, n. 67 above, at 83. See also Svetz, n. 62 above, at 428.

83 METI, *Trade Secret Management Guidelines of 2003* (as amended in 2005 and 2011).

84 *Ibid.* Note: an English translation of the Guidelines could not be found, so resort was made to summaries and descriptions of the Guidelines which seem to follow US law when strictly applied. One reason for the

system that attributes different points to various secrecy efforts related to document management, computer system management and employee management, with a score of 40–60 out of 100 being deemed sufficient. While efforts to quantify secrecy measures in this way may seem odd to attorneys who are used to a more flexible approach, the METI guidelines are designed to provide meaningful input to businesses concerning the nature and scope of reasonable secrecy measures so that fewer trade secrets will be misappropriated and more successful trade secret cases can be brought.

C. Trade secrets in employment relationships

10.126 In Japan, employees are famously loyal owing in large part to the history, culture and values of Japan, but also because of the prospect of lifetime employment for some. This strong sense of loyalty to one's employer, together with the infrequency of employee mobility, has resulted in a paucity of cases involving the alleged misappropriation of trade secrets by Japanese workers.[85] It also means that there is not a history of detailed employment agreements in Japan. But the situation has changed over the past 25 years, in part explaining the increased willingness of Japanese officials to act to protect trade secrets.

10.127 As in the United States, there are a range of employment situations and relationships in Japan, with relationships at one extreme being short term and 'at will' and at the other extreme being governed by detailed collective bargaining agreements between companies and union members. What is more prevalent in Japan than in the United States, however, is the custom and practice of long-term employment relationships.[86] Although Japanese labour law is generally based upon freedom of contract and at-will employment is the default rule, the practice of many companies is to enter into fixed-term or long-term relationships with their employees which give rise to various legal duties, including the duty to avoid abusive dismissals and the need to comply with the Japanese Labour Contracts Act. Pursuant to recent changes to the Labour Contacts Act, employees who work under a fixed-term contract for five years have the right to apply for permanent employment.[87] Under both fixed-term

perception that the METI guidelines define reasonable efforts more stringently than comparable US law is because they are in the form of advice to businesses, rather than a statement of applicable law. US attorneys who are well informed about US trade secret law are likely to give similar advice, even if there may be some cases that suggest that lesser efforts will suffice.

85 Dratler, n. 63 above, at 110–12.

86 Atsushi Tsuneki and Manabu Matsunaka, 'Labor Relations and Labor Law in Japan' (2011) 20 *Pac. Rim L and Pol'y J* 529.

87 Rodo Keiyaku Ho [Labour Contract Act], Law No. 128 of 2007, art. 18, as amended in 2012 (effective 1 April 2013) (Japan) (LCA).

contracts and open-ended (or permanent) contracts, employees can only be terminated for cause.

10.128 Despite the right of 'permanent' employment in some situations, according to the Constitution of Japan, every person in Japan has the freedom to choose his or her occupation and, thus, the right of employee mobility.[88] Given this right and the uneven bargaining power between employers and employees, Japanese officials are apt to carefully scrutinize any work rules that impose negative consequences upon employees and will interpret the employment relationship to achieve balance (or fairness). They are also apt to scrutinize any individually negotiated contracts for fairness. In other words, when it comes to freedom of contract with employees, there are more constraints placed upon employers in Japan than in the United States.

10.129 In theory, a company doing business in Japan could insist on confidentiality agreements that are typically advised between US companies and their employees (see Chapter 5 for more details), but due to the strong expectation of loyalty by employees in Japan, a duty of confidentiality will apply regardless. Pursuant to the Labour Contracts Act, employees are required to perform their employment obligation 'in good faith' and cannot abuse their rights, which includes an obligation not to disclose the confidential information of one's employer.[89]

10.130 A key question in Japan (as in the United States) concerns the parameters of applicable duties of confidentiality and whether and to what extent it applies post-employment. As a practical matter, without a written agreement, it is hard to know the extent of the obligation and to define when it begins and ends. As noted above, the trade secret administration measures that are required by Japanese law are principally designed to put the recipients of information on notice of what information should be protected as a trade secret. This can be accomplished through a written agreement or written employment rules, but may also be accomplished through the proper marking and handling of trade secret information.

10.131 Because of the expected loyalty of Japanese employees and the need to save face, practical questions arise whether an express duty of confidentiality should be requested and how detailed any written duty of confidentiality should be. Because the request for a written confidentiality agreement with employees may evidence a lack of trust that is inconsistent with forging a long-term relationship, careful consideration should be given to whether to ask for such an

88 Japanese Constitution, art. 22(1) .
89 LCA, art. 3(4)–(5),

agreement, particularly with employees that are not directly engaged in research and development efforts or who are unlikely to switch jobs.

10.132 With respect to non-compete agreements, the same concepts of loyalty that give rise to an implied duty of confidentiality underlie the rule in Japan that employees are under an obligation not to compete with their employers. Based upon the Constitutional right of employment mobility, however, this rule usually only applies during employment. Thus, express non-compete agreements are needed to bind individuals after their employment with a company. They can also be useful in defining the scope of the non-compete obligation during employment.

10.133 The enforceability of non-compete agreements has long been recognized in Japan,[90] provided that they are reasonable. The factors that have typically been considered are: (1) whether the restraint is needed to protect a legitimate business interest; (2) the position of the employee during the term of employment; (3) the extent and nature of the restraint, typically in terms of length and geographic scope; and (4) the consideration given for the restraint.[91]

10.134 Recent amendments to the METI Trade Secret Management Guidelines include a new section on 'Effectiveness of Non-Competition Agreements'. In addition to the foregoing considerations, these guidelines state that non-compete agreements are likely to be effective if they are for a period of one year or less, are limited in the scope of work that is prohibited and include extra compensation for the promise of non-competition.[92]

10.135 With respect to the issue of ownership of employee-created inventions, the law of Japan is extremely favourable to employees,[93] although pressure is being applied to Japan by the United States and various industry groups to change the applicable law. Currently, the law of Japan with respect to the ownership of employee-created inventions and the enforceability of invention assignment agreements is very similar to the law of California. In Japan, without an agreement, the invention belongs to the employee.[94] This default rule can be altered with respect to inventions that are created within the course and scope of

90 Dratler, n. 63 above, at 99.

91 *Foseco Japan Ltd*, Nara Dist. Ct, 624 Hanrei Jiho 78 (23 October 1970).

92 Blackmore and Mitsuki, *Legal Protection and Intellectual Property: Hot Topics* (February 2014), available at www.blakemore.gr.jp/doc/newsletters_e_201402.pdf.

93 Jean E. Healy, 'The Application of Japanese Article 35 regarding "Reasonable" Compensation for Patents by Employed Inventors in Syuji Nakamura v. Nichia Corporation' (2005) 17 *Pace Int'l L Rev.* 387.

94 Japan Patent Law, Law No. 121 of 1959, arts 29, 35(1).

an employee's employment, provided that such agreements are carefully drafted to be enforceable under applicable law.

10.136 Generally, inventions that are both within the scope of the employer's business and the employee's duties ('employee inventions') can be the subject of an invention assignment agreement.[95] Agreements that are outside both the scope of the employer's business and the employee's duties ('free inventions') belong to the employee and cannot be the subject of an enforceable invention assignment agreement. Invention assignment agreements are also not enforceable with respect to so-called 'business-related agreements' (those that are within the scope of an employer's business but outside the scope of an employee's duties), but the employer is entitled to a non-exclusive license to use such inventions (known as a 'shop right' in the United States).

10.137 Japan Patent Act, article 35(2) through (4) details the requirements for enforceable invention assignment agreements. Article 35(2) recognizes the ability of employers to obtain an assignment of inventions, but article 35(3) states that the employee shall be entitled to 'reasonable remuneration'. Significantly, what is reasonable is defined by article 35(4) in reference to the profits that the employer will make from the invention.

10.138 The reason why US business interests are keen to have Japanese law with respect to employee inventions changed is because article 35 of the Japan Patent Law has been interpreted and applied to require the payment of considerable sums of money to inventors, even after the employee was already compensated under an invention assignment agreement.[96] This is a consequence of the language of article 35(4) that requires remuneration based upon profit and the fact that profits are not usually known at the time an invention assignment agreement is executed. By contrast, in the United States and most other countries, even if the ownership of employee-created inventions initially defaults to the employee, it can be changed by contract that typically does not require much (if any) additional compensation beyond that which is received from employment. However, even if Japanese law is changed, it is likely that the compensation paid to inventors will be greater than is typical in the United States because such compensation is seen as necessary to incentivize invention by individuals.

95 Yoshikazu Tani, *Current Status of Employee Inventions in Japan* (Tani and Abi Law Firm, 2002), available at www.taniabe.co.jp/e/infomation/main-patent009.html.

96 See e.g., *Olympus Optical* v. *Tanaka*, Japan Sup. Ct, 1822 Hanrei Jiho 39 (22 April 2003).

10.139 Although article 35 is part of the Japanese Patent Code, like similar legal principles in the United States that were developed in patent cases, it arguably applies to some trade secrets as well. Specifically, article 35(2) and (3) speaks of 'employee inventions' (not patented inventions) and, thus, would seem to apply to so-called 'technical trade secrets' that are within patentable subject matter. Whether it also applies to other employee-generated 'business information' is another question. If not, then other provisions of law would apply to determine the ownership of employee-generated business information and, as a practical matter, it would be wise to address patentable information and other information separately in any assignment agreement because the required compensation structures may be different.

D. Trade secrets in business relationships

10.140 Japan has a long history of contract law and commercial practices to govern business relationships. Consistent with the contract formation rules of other civil law countries, a contract is formed in Japan once mutual assent occurs, without the need for a formal written contract or consideration.[97] Thus, acquiring a confidentiality agreement for information that may be disclosed both during and after a business relationship is simply a matter of establishing mutual assent. The process for doing so, however, requires an understanding of the culture and traditions of Japanese businesses.

10.141 While contracts with business associates are important and enforceable in Japan, what is much more important is the relationship between the parties. The general advice when conducting business in Japan, and particularly when negotiating contracts, is to establish relationships of trust first and negotiate the particulars of a deal second. Once trust is established, the duties of the contracting parties are often expressed through a process of clear explanation and acknowledgement. 'If used at all, written contracts are normally kept high-level, capturing only the primary aspects, terms, and conditions of the agreement'.[98] Thus, even if a written contract is used, there are many obligations of a business relationship that will not be expressed in writing. Whether put in writing or not, the important thing with respect to trade secrets is to clearly express the expectation of confidentiality and identify the information to be protected.

10.142 As a number of commentators have observed, Japanese courts will enforce trade secret rights but they tend to be very stringent in the application of the

97 John Owen Haley, 'Rethinking Contract Practice and Law in Japan' (2008) 1 *JE Asian and Int'l L* 47.
98 *Ibid.*

requirements for trade secret protection. Thus, although it is not unheard of for implied confidentiality agreements to be enforced in Japan, the better practice with respect to the need to prove reasonable efforts is to base any claim of trade secret misappropriation on an express written confidentiality agreement (or non-disclosure agreement (NDA)). If the high-level form of contract that is typical of Japanese contracting practices is used, then a general statement of duties of confidentiality with respect to the exchange of information should suffice, but the more specifics that can be negotiated the better.

10.143 Once a confidentiality agreement is entered into, an issue that arises both in Japan and elsewhere is whether the agreement only protects trade secrets or also protects a broader set of information that does not independently qualify for trade secret protection. In Japan, as in the United States, the answer to the foregoing question is 'maybe' because it depends in large part on the language and interpretation of the confidentiality agreement. If the confidentiality agreement only applies to trade secrets as defined by applicable law, then it only covers information that actually qualifies for trade secret protection. If the language of the confidentiality agreement defines a broader set of confidential information, protection of the non-trade secret information may be possible under principles of contract law.

10.144 Efforts by companies to expand the protection of information beyond that which can actually qualify for trade secret protection is controversial for at least two reasons. First, there is a fear that the language of the confidentiality agreement will cover information that is already generally known or readily accessible in contravention of the public policy that underlies those limitations on the scope of trade secret protection. Second, there is concern about the potential anticompetitive effects of restrictions on the use of information. As noted previously, while Japan is willing to protect IPRs, it recognizes their potential anticompetitive effects and, therefore, actively seeks to limit such effects. For instance, similar to US Department of Justice guidelines, guidelines have been issued by the Fair Trade Commission of Japan (JFTC) concerning the licensing of IPRs that generally recognize the pro-competitive nature of such licenses.[99] However, these licenses will be reviewed and pro-licensor provisions struck out as deemed necessary by the JFTC. Japanese courts are also likely to take matters of public interest into account when interpreting confidentiality agreements.

99 Japan Fair Trade Commission, *Guidelines for the Use of Intellectual Property under the Antimopoly Act* (2007), available at www.jftc.go.jp/en/legislation_gls/imonopoly_guidelines.files/070928_IP_Guideline.pdf.

E. Criminal consequences for trade secret misappropriation

10.145 In 2003, the UCPL was amended to include provisions for criminal penalties for the misappropriation of trade secrets for the first time. It was later amended again to extend those provisions to cover more situations and to increase the penalties for trade secret misappropriation. As currently written, the criminal provisions of the UCPL are set forth in articles 21(1) and 22. One of the reasons for the more recent amendments to the UCPL was Japan's realization that its companies are being victimized by trade secret theft. It is anticipated that, for similar reasons, the 2015 amendments will extend the criminal provisions to activities occurring outside of Japan if they have an affect in Japan.

10.146 Article 21(1) begins by stating that the criminal misappropriation of trade secrets is punishable 'by imprisonment with work for not more than ten years, a fine of not more than ten million yen, or both'. Article 21(1)(i) through (vii) describe the acts and *mens rea* that constitute criminal behaviour in a manner that is similar to article 2 of the UCPL, but including language that was specifically designed to address: (1) the actions of former officers or employees of a corporation; (2) the recipients of stolen trade secrets, including foreign governments; and (3) actions occurring outside of Japan.[100]

10.147 Article 21(i) concerns the wrongful acquisition of trade secrets by 'an act of fraud or others (which means an act of deceiving, assaulting, or intimidating a person) … or an act violating a control obligation (which means an act of stealing property, trespassing on a facility, making an unauthorized access) … or violating the control of a trade secret maintained by its holder in any other way'. Article 21(ii) through (iv) concern the wrongful use or disclosure of trade secrets under various circumstances. The first subdivision relates to disclosures or use after a wrongful acquisition. The second and third subdivisions relate to disclosures or use in breach of a duty of confidentiality. Article 21(v) through (vii) relate to the duties of officers or employees of a trade secret holder (aka owner). All of the foregoing provisions require that the bad acts be undertaken 'for the purpose of acquiring an illicit gain or inflicting a loss to its holder'.

10.148 Article 22 concerns the potential criminal liability of 'a juridical person, or an agent, employee or any other of a juridical person or an individual' who has committed a violation of article 21(i), (ii) or (vii). Such companies or individuals may be 'punished by a fine of not more than three hundred million yen'.

100 Japan Patent Office, n. 68 above, 4; Yoshikazu Iwase *et al.*, 'The Latest Amendments to the Japanese Unfair Competition Prevention Law' (2005) *JTA Bulletin* 11.

10.149 The criminal provisions of the UCPL apply to actions that take place inside of Japan and to actions occurring outside of Japan with respect to trade secrets that had been kept in Japan. This provision is designed to increase the protection afforded to trade secrets that are developed and maintained by Japanese companies.

F. Litigating trade secret disputes

10.150 The Code of Civil Procedure (CCP) of Japan applies to specify how trade secret misappropriation cases are to be commenced and litigated and were amended substantially, effective 1 January 1998, to create a 'New Code'.[101] As in the United States, civil litigation in Japan begins with the filing of a written complaint that is then served upon the defendant. The next step is for the court to set a date for oral argument (essentially the concluding part of the trial) and summon the parties to appear. Unlike in the United States, pretrial motion practice and discovery is limited. Rather (as is the case in many other countries), the facts relevant to the case are brought out at trial through the examination of witnesses and parties (although as noted below, there are special provisions within the UCPL concerning the discovery of information relevant to a calculation of damages). There is no right to jury trial in Japan and, typically, efforts to arrive at a settlement will be engaged in throughout the process.

10.151 The limited pretrial discovery methods include the ability of the parties to make inquiries by written document of their opponents, as specified by article 163 of the CCP and the possibility of preliminary oral arguments and preparatory proceedings as set forth in articles 164 and 168, respectively. In more complex cases, a 'Plan for Trial' may be developed which specifies an orderly sequence of events that may occur over a period of time and may include 'a period for advancing allegations or evidence on a specific matter'.[102]

10.152 As in the United States, Japan follows a principle of open judicial proceedings that results in both the written records of litigation and courtroom proceedings being open to the public. Article 82(1) of the Japanese Constitution provides that 'trials shall be conducted and judgment declared publicly'.[103] According to article 82(2) of the Japanese Constitution, this preference for open legal proceedings can only be overcome if a court unanimously determines that publicity would be 'dangerous to public order or morals'. When the trade secret provisions of the UCPL first came into effect, the principle of open judicial

101 Minji Soshoho [Code of Civil Procedure] 1996 (Japan).
102 *Ibid.* art. 147–3.
103 Matsuo, n. 67 above.

proceedings was applied to trade secret cases with few, if any, exceptions. When the CCP was amended, effective 1 January 1998, it improved (but did not entirely fix) the difficulty of protecting trade secrets during litigation.[104] The New Code states that there is no general duty to produce documents containing trade secrets. It also allows access to trial records to be restricted upon motion where a *prima facie* showing is made of the existence of trade secrets.[105] However, even these changes to Japanese procedure were deemed by many to be inadequate to protect trade secrets.

10.153 In 2005, Japan amended the UCPL to provide further protection of trade secrets during litigation in a manner that is more in line with the practices of US courts. Article 10 of the UCPL provides for the issuance of protective orders upon motion of a party where there is *prima facie* evidence of a trade secret. Article 11 concerns the possible rescission of protective orders when the requirements for a protective order are no longer met. Article 12 sets forth a process for trade secret owners to be notified when a request to review the case record is made with respect to cases where a protective order was issued, provided that a ruling to close the record had been made pursuant to article 92(1) of the CCP. Article 13 allows a court to review alleged trade secret material *in camera*.

10.154 Chapter VI of the UCPL (articles 23 through 31) reflects the most recent amendments and concerns 'special measures' for the protection of trade secrets during criminal proceedings. In summary, it specifies a process by which trade secret owners may prevent the disclosure of trade secrets during the various phases of a criminal prosecution.

10.155 The provisions of the UCPL concerning available sanctions for trade secret misappropriation have seen the most amendments since 1991 as the US government and various industry groups have continued to pressure Japan to improve its enforcement of IPRs. Originally comprised of a few articles, the current (2011) version of the UCPL now contains ten articles (articles 3 through 9 and 14) that address civil remedies for trade secret misappropriation and two (articles 21 and 22) that prescribe criminal penalties. Articles 10 through 13 are newer provisions of the UCPL that concern the availability of protective orders and the confidentiality of litigation proceedings.

---

104 Dario A. Machleidt, 'Japanese Trade Secret Protection: Litigants Can Feel Secure Bringing Misappropriation Claims in Japanese Courts' in 15 *CASRIP Newsletter* (Centre for Advanced Study and Research in Intellectual Property, Winter/Spring 2008).

105 Code of Civil Procedure, art. 92(1)(ii).

10.156 Articles 3, 4 and 14 of the UCPL describe the available civil remedies for unfair competition, including trade secret misappropriation. Of particular significance for trade secret owners who wish to preserve the secrecy of their information is article 3(1) which provides for injunctive relief for both the actual and likely misappropriation of trade secrets. Article 3(2) further allows for an order for the destruction of infringing goods and 'objects created by the act of infringement', which presumably would include the tangible embodiment of trade secrets. However, pursuant to long-standing procedural rules of Japan, any injunctive relief that is granted is not enforceable with contempt proceedings.[106]

10.157 The availability of damages under the UCPL must be viewed in light of the general law of Japan with respect to legal remedies.[107] Consistent with the general rules of damages in the United States, the Japanese Civil Code and general principals of tort law allow for the award of damages based upon actual loss provided that there is some causal relationship between the wrong and the harm.[108] In light of the fact that it is often difficult for companies in competitive markets to prove actual losses as a result of trade secret misappropriation, however, a broader conception of damages for trade secret misappropriation was needed. Additionally, the methods for proving such damages needed to be eased.

10.158 Article 4 of the UCPL specifies that a person who 'infringes on the business interests of another person by unfair competition shall be liable for damages'. Article 5 of the UCPL then details how such damages are to be calculated and proven. Similar to the UTSA, the UCPL adopts a broad conception of damages that, in addition to the traditional measure of damages of actual loss that is specified in the Civil Code, includes profits obtained from the sale of infringing articles (article 5(1) and (2)) and reasonable royalties for use (article 5(3)). Article 5(4) of the UCPL gives the court discretion to decrease the award if the wrongdoing was not intentional. Pursuant to article 5(2), unjust enrichment (in US parlance) is presumed to be the amount of the plaintiff's loss, but a greater amount of actual harm may be shown.

10.159 Based upon a plain reading of articles 6 through 9 of the UCPL, it is clear that they are designed to make it easier (compared with traditional rules of civil procedure in Japan) for plaintiffs in trade secret misappropriation cases to prove compensable harm and to make Japanese law more consistent with the remedies provisions of the UTSA. Article 6 is a burden-shifting provision that

106 Svetz, n. 62 above, at 432.

107 See Masumi Anna Osaki, 'A Look at Damage Awards Under Japan's Trademark and Unfair Competition Prevention Law' (1999) 8 *Pac. Rim L and Pol'y J* 489, 497 (describing traditional measure of damages).

108 *Ibid.* See also Matsuo, n. 67 above, at 93.

places the burden on the defendant to specify how the trade secrets were used or disclosed. Article 7 requires the production of documents that are necessary to calculate damages. Article 8 allows for the use of expert testimony to compute the amount of damages. Finally, in light of the difficulty of proving damages in trade secret cases, article 9 gives the courts discretion to 'determine a reasonable amount of damages based upon the overall purport of the oral arguments and the results of the examination of evidence'.

10.160 Article 14 of the UCPL reflects a unique aspect of Japanese culture. It provides that a court may order a person who engaged in acts of unfair competition 'to take those measures necessary to restore the business reputation' of the plaintiff in lieu of or in addition to the award of damages. Usually, such efforts take the form of a public letter of apology.[109]

10.161 The ability to obtain an injunction and damages for trade secret misappropriation is limited by articles 4 and 15 of the UCPL. Article 15 states that the right to request an injunction will cease if it is not exercised within three years from the time the trade secret owner becomes aware of facts giving rise to the alleged misappropriation, and that in no event will the right to obtain an injunction extend beyond ten years from the misappropriation. The last sentence of article 4 states that these same limitations apply to a claim for damages. Proposals are currently being considered in Japan to extend the ten year 'objective exclusion period' to twenty years.

10.162 The UCPL does not contain a provision that defines applicable defences to trade secret misappropriation, but article 19(vi) does specify an exception. In essence, it states that a right to request an injunction or pursue criminal sanctions does not apply to trade secrets that were acquired in good faith. Additionally, it is understood under Japanese law that the acts of reverse engineering and independent development are not acts of trade secret misappropriation. As in the United States, other provisions of Japanese law, including the Antimonopoly Act and the laws and legal principles governing employment, may also define and limit the scope of trade secret rights.

109 Svetz, n. 62 above, at 434–5.

V. MEXICO

A. Overview of the legal system

10.163 Like the legal systems of other countries, the current legal system of Mexico is the product of many influences and a history of conquests and wars, including most prominently the influences of Spanish legal principles as a result of more than 300 years of Spanish rule from 1510 to 1821. But even before Spanish rule, the legal history of Mexico reaches back centuries to the customs, practices and beliefs of its indigenous cultures, including Aztec, Mayan, Zapotec, Olmec, Huastec and Mixtec. Thus, certain pre-Hispanic norms endure, including the 'ejido' system of rules for the communal development of agricultural lands.

10.164 The Spanish conquest of Mexico in the sixteenth century brought a transplanted version of Spanish law to Mexico that was a mix of Roman, Germanic and canonical laws, royal decrees and administrative practices. The legacy of Spanish colonial law is evident in Mexico today in a number of ways. Most importantly with respect to its legal system. Like Spain, Mexico follows the civil law tradition which rejects the principle of *stare decisis*, thereby limiting the power of courts to make laws. Also, there is a centralized form of government decision-making, particularly with respect to issues of national (as opposed to local) interest.

10.165 After Mexico achieved its independence from Spain in 1821, there was a period of political turmoil and unrest, ultimately leading to the Mexican Revolution of 1901–1929 and the adoption of the fourth in a series of Mexican Constitutions in 1917. Formally known as the Political Constitution of the United Mexican States, the Constitution of 1917 still governs Mexico today. Drawing on predecessor Constitutions, this Constitution establishes 'a federal, democratic, representative Republic composed of free and sovereign states'.[110]

10.166 The Mexican Constitution of 1917 also establishes three branches of government: the executive, legislative and judicial branches. It specifies that (as in the United States) the judicial branch of Mexico consists of district courts, intermediate appellate courts (known as the Council of the Federal Judiciary), and a Supreme Court (known as the Supreme Court of Justice of the Nation). Importantly for the discussion of employee relationships, below, the Constitution of 1917 also includes a broad set of workers' rights.[111]

110 Constitucion Politica de los Estados Unidos Mexicanos, art. 40 (Mex.).
111 *Ibid*. art. 123.

10.167 The organization of government in Mexico is remarkably similar to the organization of government in the United States. The Republic of Mexico consists of 31 sovereign states and the Federation District of Mexico City (the seat of the federal government like the District of Columbia) and is spread over a wide geographic region. The governments of each of the states are organized in a fashion similar to the states of the United States with three branches of government and bicameral legislatures that share power with the federal government of Mexico.[112] The federal government of Mexico is led by the President and the chief legislative body is the Congress of Union comprised of the Senate and the Chamber of Deputies.

10.168 Because Mexico is a civil law system, the primary source of law in Mexico is written laws. The supreme law of the land in Mexico is the Constitution. Next in order of importance are the laws adopted by federal and state governments. Thus, the best source of information concerning the laws of Mexico is the Constitution and laws themselves. Mexican legal authorities will also apply custom when allowed to do so by applicable law.

10.169 Other sources of information concerning the laws of Mexico include regulations that are issued by the President of Mexico from time to time for the purpose of explaining and interpreting the laws. These are published in a document known as the Official Journal of the Federation. Additionally, it is well established in Mexico that treatises written by legal scholars are an important source for understanding the law and, accordingly, have persuasive authority.

10.170 In keeping with Mexico's civil law tradition, court decisions have little precedential value and are rarely published. However, Mexico follows a process whereby the decisions of the Supreme Court and the intermediate appellate courts can become binding on lower courts under specified circumstances that generally require five consecutive uninterrupted decisions on the same point of law. These binding rulings are published as part of the Federal Judicial Weekly.

10.171 Mexico is an active participant in the community of nations and has long agreed to protect intellectual property rights. Mexico has been a member of the Paris Convention since 1903 and the Berne Convention since 1967 (more than 21 years before the United States joined). It has been a member of the WTO since its inception on 1 January 1995 and is a member, with Canada and the United States, in the North American Free Trade Agrement (NAFTA), which went into effect on 1 January 1994. In fact, it was Mexico's agreement to the trade

112 *Ibid*. art. 115.

secret provisions of NAFTA (Article 1711) that arguably helped to resolve an impasse in the TRIPS negotiations.[113] Fourteen developing countries (not including Mexico) took the position that trade secrets were not a form of intellectual property and should not be included in the TRIPS Agreement. Mexico's concession on this point gave the United States a powerful counter-argument. However, as a developing country, Mexico was not required to fully comply with the TRIPS Agreement until 1 January 2000.

10.172 In Mexico, international treaties are not self-executing, meaning that legislation must be adopted to implement the requirements of international agreements. Thus, Mexico has adopted a number of laws in an effort to comply with its obligations under the TRIPS Agreement, NAFTA and other international agreements to which it is a party.

B. Contours of trade secret protection

10.173 The Industrial Property Law (IPL) is the Mexican federal law that governs trade secrets.[114] Some other statutes and regulations relating to confidential information as well as NAFTA (Article 1711) and TRIPS (Article 39) are also related to this area.[115] Significantly, NAFTA requires that all signatories implement laws to protect trade secrets and sets forth details about the required laws that are more extensive than what is set forth in Article 39 of the TRIPS Agreement.

10.174 Among other things, the trade secret laws of the three NAFTA countries must protect trade secrets from being misappropriated. This is defined in Article 1711.1 of NAFTA as the disclosure, acquisition or use of trade secrets by those without consent to do so or in a manner contrary to honest commercial practices. In language similar to Article 39.2 of the TRIPS Agreement, information must meet the following requirements to be protected as a trade secret: (1) it must be secret and not generally known; (2) it must have actual or potential value because of its secrecy; and (3) the owner must have taken reasonable steps to protect its secrecy.

10.175 Article 1711 of NAFTA also includes three subsections (5–7) that deal with the subject of data exclusivity (discussed in Chapter 7) and three subsections (2–4)

---

113 Sharon K. Sandeen, 'The Limits of Trade Secret Law: Article 39 of the TRIPS Agreement and the Uniform Trade Secrets Act on Which It is Based' in Rochelle C. Dreyfuss and Katherine J. Strandburg (eds), *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research* (2011), pp. 537, 546–9.

114 Ley de la Propiedad Industrial [Industrial Property Law], amended 9 April 2012 (IPL).

115 Hector Chagoya, *Trade Secrets Throughout the World: Mexico* (2014), vol. 2, para. 26:2.

that are further refinements to the general obligation to protect trade secrets. Subsections 2 through 4 of Article 1711 read as follows:

> 2. A Party may require that to qualify for protection a trade secret must be evidenced in documents, electronic or magnetic means, optical discs, microfilms, films or other similar instruments.
>
> 3. No Party may limit the duration of protection for trade secrets, so long as the conditions in paragraph 1 exist.
>
> 4. No Party may discourage or impede the voluntary licensing of trade secrets by imposing excessive or discriminatory conditions on such licenses or conditions that dilute the value of the trade secrets.

10.176 Similar to the law of the United States, not all confidential information can be considered a trade secret under Mexican law as certain conditions must be met to achieve trade secrecy. Unlike the United States (but consistent with the language of NAFTA, above), however, the IPL further requires that protected confidential information must be embodied in documents, electronic form or other tangible media.[116] Thus, Mexican law does not protect trade secrets that exist only in an individual's mind. This would include the general skill and knowledge of employees as well as ideas and inventions conceived of by individuals but never written down.

10.177 Article 82 of the IPL provides that a trade secret consists of information: (1) that has industrial or commercial application; (2) that is kept by a legal or natural person in confidence; (3) that provides a competitive advantage in the performance of economic activities; and (4) where the owner has taken sufficient means to preserve the confidentiality of the information and maintain restricted access to it. Article 82 further provides that a trade secret must be related to the nature, characteristics or purposes of a product, to methods or production processes, to means or forms of distribution of products or to the providing of services. It excludes information that is in the public domain, generally known to those in the art, public knowledge or that has been revealed by law. Information disclosed for the purpose of obtaining license permissions or registrations is not considered to be in the public domain.

10.178 In addition to the IPL, various other Mexican statutes and regulations may apply to trade secrets. For instance, article 1910 of the Federal Civil Code (FCC) provides generally that persons engaging in unlawful actions that cause damage to a third party are obliged to repair the damage unless they can prove inexcusable negligence or guilt by the damaged party. Thus, if a person acquired

116 IPL, art. 83.

a trade secret (other than through a related contract), this section may be applicable. That is because misappropriation of a trade secret is a crime under the IPL and is therefore unlawful behaviour. Arguably, if trade secret information is stolen or disclosed without the owner's consent, the owner suffers damage from loss of a competitive advantage. Also, assuming that measures were taken to maintain the confidentiality of the information, the misappropriation would not be due to the inexcusable negligence of the owner.

10.179 Another example of a general law that may apply to trade secret claims is article 1882 of the FCC. It states that '[h]e who without cause enriches himself to the detriment of another is obliged to indemnify the latter for the latter's impoverishment to the extent he enriched himself'.[117] It provides for an unfair enrichment claim that, under the right factual circumstances, might apply to the unauthorized use of trade secrets through misappropriation or through a breach of contract. One could argue that a person or entity that received an unfair competitive advantage from a trade secret belonging to another party has been unjustly enriched by the proprietary knowledge to the detriment of the trade secret owner.

C. Trade secrets in employment relationships

10.180 Mexico's Federal Labour Law (FLL),[118] governs employment relationships in Mexico and gives Mexican workers significant rights. Nonetheless, article 134 provides that employees have an obligation to maintain the confidentiality of any technical, commercial and manufacturing secrets used in the manufacture of products in which they are directly or indirectly involved, as well as any confidential business information of the employer disclosure of which might harm the company. Furthermore, article 47(IX) of the FLL provides that an employer may terminate a contract with an employee if the employee reveals secrets or private information belonging to the employer. Thus, the disclosure of confidential information by an employee is an illegal act in Mexico that can be enforced through the civil and criminal codes. While the protections governing confidential information in the FLL are broader than those provided for trade secrets in the IPL, the FLL applies only to employees in a strict sense. Thus, if the offender is a former employee the FLL does not apply.

10.181 Article 85 of the IPL provides that any person who by virtue of his position obtains access to a trade secret which he knows is proprietary or confidential must refrain from disclosing it without the consent of the owner. The article

117 Codigo Civil Federal [Federal Civil Code], art. 1882.

118 Ley Federal de Trabajo [Federal Labour Law], as amended 30 November 2012.

also provides that any person or company hiring an employee or former employee of a third party or consultant for the purpose of acquiring the trade secrets of the third party will be responsible for payment of damages. Thus, even if an employment contract does not contain a confidentiality clause, the employee has an obligation implied under the FLL to maintain the confidentiality of trade secrets.

10.182 Despite the foregoing, as is stressed throughout this book, it is important to clarify in an employee's contract that the employee will have access to confidential information, that the information should remain confidential and to remind the employee of the obligations under the IPL, FLL and the FPC regarding confidential information. It is also important that the employee acknowledge receipt of each piece of confidential information to which he has access during his employment as this will help with enforcement efforts, if necessary.

10.183 It is common practice in Mexico to provide a termination letter containing a statement by the former employee that she has received payment according to the employment contract, that the employer does not owe the employee any further compensation and that all pending obligations between the employer and employee have been met. These letters should, but rarely do, contain statements regarding access to and protections for the confidential information of the employer. To prevent potential disclosure after employment and establish the circumstances for enforcement under the criminal law and the IPL, it is recommended that departing employees receive such notice.

10.184 In general, covenants not to compete are not valid in Mexico. This is because they are contrary to the Constitutional right to liberty of work. Article 5 of the Mexican Constitution provides that 'no person can be prevented from engaging in the professional, industrial, or commercial activity or occupation of his choice'.[119] The exception is that a judicial order may issue when the rights of third parties are infringed or if the rights of society are violated.[120] Thus, the law requires proof of trade secret misappropriation before an order from a court preventing competing activity can be obtained.

10.185 The Mexican Constitution further provides that any agreements compelling a person legally to agree on his 'own banishment or exile, or to the temporary or permanent renunciation' of the performance of his professional, industrial or commercial activity is void.[121] Similarly, article 4 of the FLL provides that a

119 Constitucion Politica de los Estados Unidos Mexicanos, art. 5(1).
120 *Ibid.*
121 *Ibid.* art. 5(5).

person shall not be prevented from obtaining a job or participating in a profession, industry or branch of commerce of his choice if they are lawful. Therefore, private contracts containing non-compete provisions are void. However, Mexican employers often include restrictive covenants and confidentiality agreements as part of employment agreements.[122] The employer then has grounds to dismiss an employee who violates the provisions without having to make a severance payment to the employee.

10.186 Regarding ownership of inventions, article 9 of the IPL specifies rules that are identical to the law of the United States in that the default rule is that any natural person who develops an invention shall have the exclusive right to exploit it. Article 14 of the IPL provides that the FLL shall apply to inventions of persons involved in an employer-employee relationship. However, where the employee was hired to perform work related to research or development for the employer, the employer will own the invention. Similar to the law of the United Kingdom, when the importance of the invention and the benefit to the employer is out of proportion as compared to the regular compensation to the employee, the employer is required to pay the employee an additional amount. In any other case, the employee who developed the invention will own it, but the employer will have a preferential right to obtain an exclusive license or to acquire the invention (this is similar to a 'shop right', discussed in Chapter 3).

D. Trade secrets in business relationships

10.187 Importantly for companies doing business in Mexico, Mexico's IPL expressly contemplates holding companies liable for trade secret misappropriation. Article 86 states that any 'company engaging [a worker, professional, or consultant] … with a view to obtaining trade secrets … shall be liable for payment of damages'.[123] It also provides that a company that obtains trade secret information through unlawful means shall similarly be liable for damages.

10.188 The licensing of a trade secret is permitted under article 84 of the IPL. These licenses and other agreements containing confidentiality clauses must clearly identify the trade secrets. Also, the parties may agree on a punishment in case of a breach. However, if the affected party relies on this contractually specified penalty (akin to a liquidated damages clause), it is no longer entitled to claim actual damages. On the plus side, such a clause eliminates the need to prove

122 See Monica Schiaffino, 'Protecting Employers' Trade Secrets and Confidential Information in Mexico' in *Practical Law Multi-Jurisdictional Guide 2013/14*.

123 IPL, art. 86.

damages, requiring the trade secret owner only to prove breach of the agreement. Thus, Mexican lawyers often prefer to use these penalty provisions and agreements.[124]

10.189 Mexican law further provides, under article 2028 of the FCC and the Civil Code for the Federal District (CCFD), that a person who promises to refrain from doing a particular action and does not comply with his obligation will be subject to the payment of damages. This would apply to the breach of a confidentiality clause and a promise not to disclose a trade secret.

10.190 The laws applicable to technology licensing (which could include trade secrets) are included in the IPL, which also governs other forms of intellectual property rights in Mexico, including industrial secrets, patents and trademarks.[125] It does not require any specific formalities for parties to enter into a binding agreement. However, in order to ensure enforcement against third parties, the agreement should be registered with the Mexican Institute of Industrial Property. Registration is also recommended so that the parties may be able to have the benefits associated with the licensed technology. To allow for registration, the agreement must provide that Mexican law will govern the interpretation and enforcement of the agreement, unless none of the parties are domiciled in Mexico.

10.191 Since Mexican law does not recognize the remedy of specific performance for breach of contract, a license agreement should be very clear on the grounds for termination of the license and the procedures for determining responsibility for termination in order to determine appropriate remedies. Otherwise, it is generally assumed in Mexico that a licensee will enjoy free use of the licensed technology once the license agreement is terminated. If the licensor does not intend that to be the case, specific language should be put in the agreement to make it clear that the rights to use the technology will cease when the agreement expires.

10.192 Specifically related to franchise agreements, article 142*bis*(2) of the IPL obligates franchisees to maintain confidentiality of confidential information during the term of the agreement and beyond the term of the agreement. Furthermore, all professionals in all areas are obligated to maintain the secrecy of any business information received from a client.[126]

---

124 Chagoya, n. 115 above, para. 26:8.

125 IPL, art. 136.

126 Regulatory Law of the 5th Constitutional Article, on Professional Performance in the Federal District, art. 36.

E. Criminal consequences for trade secret misappropriation

10.193 The unauthorized disclosure of confidential information or a trade secret is a crime in Mexico if there is intent or purposeful use or disclosure. Article 223 of the IPL contains three categories of trade secret crimes: (1) disclosing a trade secret without the consent of the owner with knowledge that it was confidential and for the purpose of obtaining economic benefit or causing harm to the owner of the secret; (2) misappropriating a trade secret without the consent of the owner for the purpose of using or revealing it and obtaining economic benefit of causing harm to the owner; and (3) using a trade secret without the consent of the owner for the purpose of obtaining economic benefit for oneself or causing harm to the owner.

10.194 Disclosure of confidential information can also constitute a crime even if it does not meet the criteria for trade secrecy described above. Article 210 of the Federal Penal Code (FPC) provides that any person who reveals a secret received by virtue of his employment or position will be punished with 30 to 200 working days of community service.[127] The disclosure must have been without fair cause and without the consent of those who are affected by the disclosure. Article 211 of the FPC makes a person who provides professional technical services or as a government employee liable for up to five years in prison and a fine of 50 to 500 Mexican pesos for making an unauthorized disclosure of confidential information.

10.195 Penalties under article 224 of the IPL include two to six years in prison and a fine of 100 to 10,000 times the daily wage applicable in Mexico City. This penalty is independent of damages that a trade secret owner may be able to recover under article 221*bis* (minimum of 40 per cent of the net sale price of products or services sold using the trade secret).

10.196 If an action is filed under article 223 of the IPL, the case must be initiated before the Federal Prosecution Agency which will then investigate and refer the case to a criminal court. In Mexico City, there is a Special Agency for IP Crimes of the Federal Prosecution Agency.

F. Litigating trade secret disputes

10.197 Civil, administrative and criminal actions can be initiated concurrently to enforce trade secret rights in Mexico. According to article 227 of the IPL, trade

127 Codigo Penal Federal, art. 210.

secret actions may be brought in any federal court in Mexico. Local courts may also hear trade secret cases if private contracts between the parties so provide.

10.198 The laws in Mexico do not provide specifically for injunctions in trade secret and other IPR cases. This may be due to the fact that, historically, industrial property litigation in Mexico was handled administratively rather than through judicial action. Thus, law-makers may not have appreciated the significance of preliminary relief for litigants. Accordingly, unlike in the United States, there is not much of an opportunity in Mexico for preliminary injunctive relief to restrain an employee or business partner from violating a restrictive covenant or misappropriating trade secrets.

10.199 While there are some limited circumstances under which a claimant in a civil court action may seek an injunction to attach or seize goods, it is thought to be unlikely that such limited circumstances would apply to trade secret cases, given the rarity of such injunctions. There is also a provision permitting the Mexican Institute for Industrial Property to seize goods used in the performance of a crime under article 211 of the IPL. However, it is believed to be unlikely that this provision would be utilized for trade secrets.

10.200 The Mexican Institute for Industrial Property is empowered to conduct administrative proceedings involving the violation of rights and to impose sanctions.[128] More specifically, article 213 of the IPL also classifies as an administrative infringement any act 'contrary to proper practice and custom … which amount[s] to unfair competition'.[129] In general, administrative authorities in Mexico tend to have broad powers, among other things, to make final decisions, order that a party stop infringing and order payment of damages and attorney's fees. Similar to judicial proceedings, parties to administrative proceedings can also be bound by the equivalent of US protective orders, protecting and preventing disclosure of trade secrets revealed during such proceedings.[130]

10.201 Damages may be recovered in a civil action in addition to criminal penalties. Indeed, article 226 of the IPL provides that '[r]egardless of the institution of criminal proceedings, the aggrieved party in any of the offenses [covered under the IPL] may demand … compensation and the payment of damages'. Further clarification on the amount of damages is set forth in article 221 of the IPL. It provides that an aggrieved party is entitled to at least 40 per cent of the net sale price of the products or services that embody the misappropriated trade secret.

128 IPL, arts 214–215.
129 *Ibid*. art. 213.
130 See *ibid.* art. 86*bis*(1).

10.202 Confidential and trade secret materials submitted for a trial or proceeding may be marked and kept confidential in compliance with article 14 of the Law on Transparency and Access to Governmental Public Information.[131] In order to avoid disclosure at the end of a civil trial, the trade secret owner should expressly request that the judge or government authority keep the information confidential indefinitely. Furthermore, as indicated above, where a party receives trade secret information during a judicial or administrative proceeding, the party is required to take measures to prevent disclosure of that information to third parties.[132]

131 Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, art. 14.
132 *Ibid.*

APPENDIX 1: COMPARISON OF THE UTSA AND THE PROPOSED EU TRADE SECRET DIRECTIVE

I. INTRODUCTION

A1.01 Given its potential geographic scope throughout the European Union, this Appendix analyses the proposed '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 dated 28 November 2013.[1] Also reflected in this analysis are the amendments to the proposed Directive by the Council of the European Union.[2] A redlined copy of the initial proposal showing the Council's amendments and additions is provided in Appendix 2. Collectively, these documents are referred to throughout as the 'EU Trade Secret Directive' or 'the Directive'.

A1.02 Although it is unclear as of mid-2015 if and when the Directive will be approved by the European Parliament, pursuant to statements that were made when it was introduced, the goal is to have it enacted and fully implemented by EU countries by late 2018 (five years after its introduction). Unless this goal is altered, this means that all EU countries will be required to amend their existing trade secret laws to conform to the Directive.[3] It also means that statutory law,

1 European Commission, *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*, 2013/0402 (COD) (2013), reprinted as amended in Appendix 2.

2 Council of the European Union, 9870/14.19 (May 2014).

3 See Consolidated Version of the Treaty on the Functioning of the European Union (TFEU), art. 114, [2010] OJ C83/47.

rather than common law, may become the primary source of trade secret law in the United Kingdom and other common law countries within the EU.

A1.03 In countries that already have robust trade secret protection laws and principles as described by the European Commission Study first discussed in Chapter 1,[4] no change in existing trade secret law may be necessary as a result of the Directive (for example, in Sweden), but for other countries the changes may be significant. In keeping with the discussion of the varied legal traditions of common law versus civil law countries (see Chapters 9 and 10), it is anticipated that the Directive will result in more codified trade secret laws that should be easier for attorneys to find and which, as described below, should be fairly consistent with US law.

A1.04 As described in the European Commission Study,[5] the various countries of the EU currently have a variety of models (including both 'dedicated' and 'general' legislation) for the protection of trade secrets, with Sweden being the only EU country with ad hoc legislation (like the Uniform Trade Secrets Act (UTSA)) that is solely addressed to trade secrets. A number of countries (Austria, Germany, Poland and Spain, for example) cite their laws governing unfair competition as meeting the TRIPS Agreement obligations to protect trade secrets.

A1.05 The EU countries of Italy, France and Portugal have specific provisions regarding the protection of trade secrets within their Codes of Industrial Property. In countries that do not have specific legislation on the topic (often because they follow a common law tradition), some trade secret principles are based primarily upon principles of tort law (the Netherlands) while others are based upon principles of tort and contract law (United Kingdom, Ireland and Malta). The European Commission Study also notes that most EU countries (with the exception of Cyprus, the Czech Republic, Ireland, Luxemburg, Malta and the United Kingdom) have specific provisions on trade secrets in their national labour laws or in their Civil Codes. Further, most EU countries (not including Bulgaria, Ireland, Malta and the United Kingdom) have criminal laws specifically devoted to trade secret violations.

A1.06 As indicated in the foregoing table of contents for this Appendix, the examination of the Directive is organized in accordance with the discussion of the

4 European Commission, *Study on Trade Secrets and Confidential Business Information in the Internal Market*, available at http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_final-study_en.pdf.

5 *Ibid.* 4–9.

UTSA in Chapter 3 so that a comparative analysis of the two sets of law can be conducted. As will be seen, both the Directive and the UTSA are substantially similar, but there are a number of differences worthy of note. Some of these differences reflect legal principles that are an ancillary part of US trade secret law but which are not expressly stated in the UTSA. Others reflect differences between US trade secret law and the Directive and, therefore, raise issues about which approach is preferable. In particular, it is important to note that the Directive contains many express limitations on the scope of trade secret protection and a number of public interest exceptions, as discussed further below.

II. A BRIEF DESCRIPTION OF THE EUROPEAN UNION

A1.07 For lawyers who are unfamiliar with the history, structure and purpose of the European Union (EU), it is important to first understand the purpose and meaning of an EU Directive and a little bit about the EU itself. Initially, dating back to a series of international agreements that were entered into in the 1950s (including the Treaty of Rome Establishing the European Economic Community (originally known as the 'EEC Treaty' but now known as the Treaty on the Functioning of the European Union (TFEU)), there were six initial members of what was then known as the European Economic Community (EEC): Belgium, France, Germany, Italy, Luxembourg and the Netherlands. Since 1958 when the EEC Treaty originally became effective, it has been amended numerous times, including in 1992 when the EU Treaty (Maastricht Treaty) was adopted (effective 1 November 1993) and in 2007 with the Treaty of Lisbon (Treaty on the European Union, effective 1 January 2009).

A1.08 As of mid-2015, there were 28 EU countries which, in addition to the original six EEC countries listed above, include: Austria, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, Greece, Hungary, Ireland, Latvia, Lithuania, Malta, Poland, Portugal, Romania, Slovenia, Slovak Republic, Spain, Sweden and the United Kingdom. The countries of Iceland, Liechtenstein, Norway and Switzerland are not members of the EU but they are members of the European Free Trade Association (EFTA).[6] Additionally, all of the EU countries, plus Iceland, Liechtenstein and Norway are members of the European Economic Area (EEA).[7] Importantly for trade secret purposes, the EEA has a provision (Article 28) concerning the freedom of movement for workers.

6 See Convention Establishing the European Free Trade Association (EFTA), 4 January 1960, 370 UNTS 3.
7 See Agreement on the European Economic Area [1994] OJ L1/3.

A1.09 The EU is a signatory to the WTO Agreement, including the TRIPS Agreement, as are all individual countries of the EU. Thus, the EU and its Member States are already obligated to comply with Article 39 of the TRIPS Agreement and to notify the WTO of the laws that they contend demonstrate their protection of undisclosed information.

A1.10 With respect to the proposed EU Trade Secret Directive, the establishment of the EU is important because pursuant to its provisions the sovereignty of Member States is altered in certain respects, particularly as it relates to trade with countries that are located outside of the EU.[8] In this regard, the EU acts in a manner similar to the US federal government with respect to its 'exclusive competence' over foreign trade and other specified matters (including in the EU's case, competition rules and commercial policy).

A1.11 Generally, the EU (through the auspices of the European Parliament) exercises its exclusive or shared legislative competencies by adopting Regulations or Directives. Regulations, once approved, have the force of law throughout the EU and are self-executing. In contrast, Directives are not self-executing and instead 'direct' EU Member States to adopt laws that comply with each Directive, leaving the exact structure and wording of those laws to the discretion of each country. The interpretation and implementation of national laws adopted to comply with EU Directives are matters for the courts of each country, but are subject to review for compliance with EU law by the European Union's Court of Justice.

III. EU TRADE SECRET DIRECTIVE COMPARED TO THE UTSA

A1.12 The proposed Directive contains two parts: an Explanatory Memorandum (EM) and the language of the Directive itself. The Directive also consists of two parts: a Preamble in the form of 28 statements of purpose (expanded to 32 by the EU Council amendments) followed by text of the Directive expressed in Chapters I through IV and Articles 1 through 20. The following is an explanation of Chapters I through III of the Directive with reference to the EM and the Preamble as appropriate.[9] Each provision of the Directive that is discussed is also compared with US trade secret law. Chapter IV of the

8 See TFEU, Pt I, tit. I.

9 For another analysis of the proposed Directive, see Comments of the Max Planck Institute for Innovation and Competition of 3 June 2014, which is generally supportive of the proposal but includes suggested changes to various provisions of the draft Directive.

Directive is not discussed because it concerns administrative and enforcement matters related to the Directive itself, and not the substantive provisions of the Directive.

A1.13 The 'redlined version' of the Directive that is included in Appendix 2 provides a useful illustration of the concerns that resulted in the EU Council amendments to the Directive as initially proposed. Significantly, it no longer requires perfect harmonization among EU Member States but, instead, authorizes 'more far-reaching protection against the unlawful acquisition, use or disclosure of trade secrets than that required in this Directive, provided that compliance with Articles 4, 5, Article 6(1), Article 7, the second subparagraph of Article 8(1), Articles 8(3), 8(4), 9(2), Articles 10, 12 and Article 14(3) is ensured'.[10] In other words, more stringent trade secret laws are allowed as long as the built-in safeguards are respected. Thus, for instance, since the Directive does not mandate the adoption of criminal laws concerning trade secret misappropriation, EU Member States would have the ability to enact such laws if they wish.

A1.14 Additionally, the Directive as amended by the EU Council includes a clearer and more numerous list of safeguards, particularly in the form of explicit exceptions to trade secret protection and enforcement. In this regard, paragraph (10)(a) through (10)(c) were added to the Preamble to describe intended limits on the scope of liability for trade secret misappropriation, as further described below.

A1.15 Overall, the justifications for the Directive provided in the both the EM and the Preamble are very reminiscent of the arguments that were made during the drafting of the Uniform Trade Secrets Act (UTSA).[11] Aside from the general belief that increased trade secret protection will spur economic development and innovation, there is an underlying desire for more uniformity with respect to: (1) the definitions of a trade secret and misappropriation; (2) the nature and scope of available remedies, including preliminary relief (or interim measures); and (3) the liability of third parties.[12]

A. Trade secret subject matter and other definitions

A1.16 The Directive begins in Article 1 with the statement that '[t]his Directive lays down the rules on the protection against unlawful acquisition, disclosure and

10 Council of the European Union, 9870/14, art. 1.

11 See Sharon K. Sandeen, 'The Evolution of Trade Secret Law and Why Courts Commit Error When They Do Not Follow the Uniform Trade Secrets Act' (2010) 33 *Hamline L Rev.* 493; Sharon K. Sandeen and Elizabeth A. Rowe (eds), *Trade Secrets and Undisclosed Information* (2014).

12 Council of the European Union, 9870/14.19, Preamble, paras (5) and (6).

use of trade secrets'. Article 2 then defines four terms. Consistent with US law, the protectable subject matter is broadly defined as 'information and know-how', provided that it meets three requirements for trade secrecy: secrecy (not generally known or readily accessible); commercial value; and reasonable steps to keep the information secret. As explained in paragraph (1) of the Preamble, the theoretical definition of a trade secret covers 'a diversified range of information, which extends beyond technological knowledge to commercial data such as information on customers and suppliers (which may involve personal data), business plans or market research and strategies'. Throughout the Directive it is stated that trade secret information may include 'know-how', but this term is not defined. As in the United States, presumably it means information that has not yet been recorded in tangible form and, thus, there is no tangibility requirement for trade secret protection.

A1.17 Paragraph (8) of the Preamble further elaborates on the definition of a trade secret. In pertinent part, and again consistent with US law, it states that the commercial value of the information can be 'actual or potential'. However, it further defines commercial value to include harms that the person lawfully controlling the trade secrets would suffer if the information is wrongfully acquired, used or disclosed, including undermining 'his or her scientific and technical potential, business or financial interests, strategic positions or ability to compete'. This appears to be a departure from the UTSA definition that requires the information to 'derive independent economic value … from not being known by others', although evidence of independent economic value in the United States is often presented in terms of the harms that the trade secret owner will suffer.

A1.18 Another difference between the Directive and the UTSA (including its commentary) is the explicit recognition in paragraph (8) of the Preamble that the definition of a trade secret under EU law 'should exclude trivial information and should not extend to the knowledge gained by employees in the normal course of their employment'. Although, as explained in Chapters 3, 4 and 5, these same limitations exist under US law, they are a product of well-established judicial decisions rather than statutory language.

A1.19 The remaining definition provisions of the Directive are different from the definition provisions of the UTSA (section 1). However, the meaning of 'misappropriation' and 'improper means' that are defined in the definition section of the UTSA are also included in Article 3 of the Directive as discussed, above. What the Directive adds that the UTSA does not have are definitions of 'trade secret holder', 'infringer' and 'infringing goods', although such definitions are generally consistent with US law.

A1.20 Under Article 2(2) of the Directive, the complainant need not be the owner of the subject trade secrets, but can be 'any natural or legal person lawfully controlling a trade secret'. The EM states that the definition of 'trade secret holder' was intended to apply to both the owners and licensees of trade secrets.[13] This is a helpful provision that will help prevent issues of standing to sue that have been known to arise in the United States; however, as noted in Chapter 4, it is generally advised that standing to sue be addressed in any agreement by which trade secrets are licensed. In the absence of such an agreement, there is case precedent in the United States that has allowed licensees of trade secrets to sue for misappropriation.

A1.21 Both the definition of 'infringer' and 'infringing goods' in Article 2 of the Directive are interesting from a US perspective because, under US law, the terms used are 'misappropriator' and 'misappropriated goods'. Thus, US lawyers often speak in terms of 'trade secret misappropriation' rather than 'trade secret infringement'. This is done, in part, as a result of happenstance but also to distinguish trade secret claims from other intellectual property (IP) claims by highlighting that trade secret rights are not exclusive rights but are only protected against misappropriation. Despite the words used in the Directive, however, it is clear that trade secret rights are not exclusive rights under the Directive. Paragraph (10) of the Preamble states: 'In the interest of innovation and to foster competition, the provisions of this Directive should not create any exclusive right on the know-how or information protected as trade secrets'. As noted in comments by the Max Planck Institute, although this distinction does not have much substantive relevance, it 'plays a role in the complementary application of the [EU] Enforcement Directive 2004/48/EG … and the determination of the applicable law under the Rome II Regulation ….'.[14] Significantly with respect to the Enforcement Directive, it is arguably inapplicable because trade secrets are not treated as 'intellectual property'.

A1.22 A definition of 'infringing goods' or even 'misappropriated goods' is not contained in the UTSA and is not a well-developed concept under US law. This is undoubtedly due to the fact that many goods reveal their associated trade secrets once they are sold in the market, thereby destroying the trade secret status of the revealed information. Conceptually then, such 'infringing goods' are usually going to be made using unrevealed trade secrets, most likely hidden processes. The definition in the Directive is actually broader because it includes 'goods whose design, quality, functioning, manufacturing process or marketing significantly benefits from trade secrets unlawfully acquired, used or disclosed'.

13 *Proposal for a Directive*, n. 1 above, Explanatory Memorandum, p. 7, para. 5.1.

14 Comments of the Max Planck Institute for Innovation and Competition of 3 June 2014, para. 12, p. 4.

This appears to be consistent with how the US International Trade Commission (ITC) (discussed in Chapter 6) and US Customs interpret trade secret misappropriated goods for purposes of border enforcement and the jurisdictional language of the US Economic Espionage Act. All such language reveals an effort to extend trade secret claims beyond the trade secrets themselves to include products made using misappropriated trade secrets.

A1.23 The term 'significantly benefits' is not defined in the Directive, meaning that the definition of infringing goods may apply to goods, the majority of which are not the result of illicit trade secret usage. Paragraph (17) of the Preamble explains that a significant benefit includes situations where the trade secret has 'a significant impact on the quality, value or price of the resulting good or on reducing the cost, facilitation or speeding up its manufacturing or marketing processes'. However, unless narrowly applied, when coupled with the Directive's seizure remedy, discussed below, the definition of infringing goods provides trade secret holders with a powerful weapon that is rife for potential abuse unless policed by judicial authorities. This is on top of the injunctive and damages remedies that are provided for in the Directive.

B. Requirements for trade secret protection

A1.24 Article 2(1) of the Directive sets forth the definition of a trade secret in a manner that is word for word identical to the language of Article 39.2 of the TRIPS Agreement. As previously noted in Chapter 2, there are some differences (mainly in word variations) between this language and the definition of trade secrets under the UTSA that may result in differences in the way the Directive is applied.

A1.25 As stated in the Directive, to be a trade secret the subject information 'must not be generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question'. Conceptually, this is a broader conception of 'prior art' than just information that is publicly known because, like US law, the subject information may not be protected as a trade secret even if it is only known within a particular industry. Interestingly, the commentary to UTSA, section 1, defines 'generally known' in this broad fashion, whereas the Directive includes it as part of the wording of the definition itself.

A1.26 Unlike the UTSA, but consistent with the TRIPS Agreement, the Directive uses the language 'not readily accessible' instead of 'not readily ascertainable'. Although this may simply reflect a difference in terminology rather than a difference in meaning, based upon the *Oxford English Dictionary* definitions of

both terms, 'accessible' appears to be a broader concept than 'ascertainable'. Although both words are adjectives, the word 'accessible' means 'able to be reached or entered', whereas the word 'ascertainable' means 'to find out something for certain'. Thus the definition of accessible under the Directive appears to be broader than the definition of ascertainable under the UTSA, meaning that less information can be a trade secret under the Directive than under the UTSA. How much less is the critical question.

A1.27 Consistent with the language of Article 39.2 (but not with the express language of the UTSA), Article 2(1)(a) of the Directive appears to limit the applicable prior art (what is generally known or readily accessible) to information that can be found 'as a body or in the precise configuration and assembly of its components'. Apparently, this qualification was added to the TRIPS Agreement due to concerns that the generally known or readily accessible limitation on protectable information would be applied too broadly to situations where the individual component parts of a product or process are well known, but where the precise combination of those known elements is not. What this qualification will mean in actual practice within the EU, however, is unclear. As discussed in Chapter 3, a theory exists under US law for the protection of so-called 'combination trade secrets', but the theory is limited and arguably extends only to the added or novel features of the combination.[15]

A1.28 Article 2(1)(b) is consistent with the language of Article 39.2 in requiring that information must have 'commercial value' to be protected as a trade secret, but nowhere in the text of the Directive or the TRIPS Agreement is commercial value defined. Presumably, the requirement means that the information must have commercial value in the sense that it could be sold or licensed to another or could be used to make the information holder's products more desirable or its processes more efficient. Notably, to qualify for protection, the information must have commercial value 'because it is secret', meaning that the secrecy provides the added value and not some other feature of the information. For instance, a compilation of information may be valuable to a company because of the efficiency of purchasing the compilation rather than the company having to compile it itself, but the compilation would not be valuable 'because of its secrecy' if the compiled information was generally known or readily accessible. Also, as noted above, there is language in paragraph (8) of the Preamble to suggest that commercial value may be evidenced by the harm that the trade secret owner suffers as a result of a trade secret misappropriation.

15 See Tait Graves and Alexander Macgillivray, 'Combination Trade Secrets and the Logic of Intellectual Property' (2004) 20 *Santa Clara Computer and High Tech LJ* 261.

A1.29 The language of Article 2(1)(b) differs from similar language in the UTSA which requires that to be protected as a trade secret, the subject information must (1) derive independent economic value (2) because it is secret from others. Whether the use of the term 'economic value' instead of 'commercial value' is a distinction with a difference is a point of contention under US law, but based upon the drafting history of the UTSA and the common law of the United States, it appears that the requirement relates to whether the information actually adds to the information holder's bottom-line from an accounting point of view rather than from an economist's point of view. In other words, the economist's conception of wealth enhancement to include psychic or other non-monetary benefits does not count. Instead, consistent with the common law of torts in the United States and elsewhere, the focus is on whether there is something of monetary value that is worth the expense of court intervention.

A1.30 The third requirement for trade secret protection under the Directive is also identical to the language of Article 39.2 of the TRIPS Agreement and is consistent with the language of the UTSA. It provides that the subject information must have been 'subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret'. The 'person lawfully in control of the information' is defined in Article 2(2) of the Directive as 'the trade secret holder'. As noted above, this would include the licensee of trade secret assets. The UTSA does not have a similar provision, but common law rules of standing in trade secret cases in the United States generally allow licensees of trade secrets to sue for misappropriation.

C. Definition of misappropriation

A1.31 The definition of misappropriation under the Directive, like the similar definition under the UTSA, goes beyond the cursory treatment in Article 39 of the TRIPS Agreement to identify a number of different wrongful acts. Similar to the UTSA, the focus of Article 3 of the Directive is on the wrongful *acquisition*, *use* or *disclosure* of trade secret information, but there are unique provisions in Article 3 that are worthy of note.

A1.32 Article 3(2) focuses on the wrongful acquisition of trade secrets by defining two (originally six) types of acquisition that are considered unlawful if engaged in without the consent of the trade secret holder. The first type concerns the unauthorized access to or copying of 'documents, objects, materials, substances or electronic files … containing the trade secret or from which the trade secret can be deduced'. This is similar to the wrongful acquisition prong of the UTSA's definition of misappropriation (section 1(2)(i)), but is more detailed in

identifying 'unauthorized access' and 'copying' as particular methods of wrongful acquisition.

A1.33 In the United States, the foregoing two methods of wrongful acquisition raise additional issues. With respect to unauthorized access, a claim for relief may also be available under the Computer Fraud and Abuse Act.[16] With respect to the alleged wrongful copying, copyright pre-emption issues may arise that require pursuit of a copyright infringement claim instead of a trade secret misappropriation claim.[17] Whether similar issues arise in the EU depends upon the non-trade secret laws of EU countries which are not explicitly pre-empted by the Directive.

A1.34 The second type of wrongful acquisition contained in the Directive (after it was amended by the EU Council) is similar to the definition of 'improper means' under the UTSA, but without any illustrative examples. Rather, Article 3(2)(f) of the Directive (presumably to be re-lettered as 3(2)(b) in the adopted version) is a broad catch-all which borrows from the language of the TRIPS Agreement in making 'any other conduct, which under the circumstances, is considered contrary to honest commercial practices' a form of wrongful acquisition. Similar language is not included in the UTSA but it is understood under US law that the definition of 'improper means' is illustrative only and was not meant to exclude other means that may be deemed improper pursuant to prevailing standards of business ethics.

A1.35 For the most part, the broad definition of wrongful acquisition under the Directive is consistent with the meaning and application of wrongful acquisition under US law, although it remains to be seen how broadly the language 'contrary to honest commercial practices' is defined and whether it will include acts that are not independently tortious or criminal. As discussed in Chapter 3, it is generally thought that under US law the improper acquisition of trade secrets can include unethical acts that are not otherwise criminal or tortious. The use of the term 'contrary to honest commercial practices' both in the Directive and in the TRIPS Agreement gives countries a lot of flexibility to define wrongdoing as they see fit.

A1.36 In the Directive as originally proposed, there was a specific *mens rea* (or intent) requirement specified in Article 3(2), but it was deleted at the EU Council level. As explained in the Introduction to the Council's comments:

16 18 USC s. 1030.
17 See 17 USC s. 301.

> Member States discussed on the conduct that should be considered as an unlawful acquisition, use and disclosure of a trade secret (Article 3). It resulted from this discussion that, while an element of dishonest behaviour would be needed, no intentionality or gross negligence criteria should be required for the unlawful conduct to exist in the case of primary infringers (e.g., the one that takes steps to acquire the information, the one that breaches a confidential duty); however, in principle a knowledge criterion should be required in the case of passive receivers of information (third parties) for their conduct to be unlawful.[18]

The foregoing explanation of the intent requirement is generally consistent with US law. Implicit in the definition of 'improper means' under the UTSA, which includes a litany of wrongs, is an obvious level of volition above negligence. The question whether the misappropriator knew or had reason to know of the existence of trade secrets is a separate issue which, according to the Directive, will determine if dishonesty is involved. It is also consistent with the UTSA for the Directive to require that third parties have knowledge.

A1.37 Article 3(3) of the Directive defines the unlawful use or disclosure of trade secrets in terms of three acts. Consistent with the definition of misappropriation under the UTSA (but expressed more simply), the first *wrongful, disclosure or use* occurs when the information that is disclosed or used was acquired unlawfully. Secondly, *wrongful disclosure* occurs when it is 'in breach of a confidentiality agreement or any other duty not to disclose the trade secret'. Finally, *wrongful use* occurs if it is 'in breach of a contractual or any other duty to limit the use of the trade secret'. What the 'other duties' not to disclose trade secrets or limit their use are and how they arise are not defined and, presumably, will depend upon the legal principles of each EU country. In other words, some EU countries may not recognize implied agreements to the extent they are recognized in the United States. This highlights the need for trade secret owners to obtain written confidentiality agreements whenever possible.

A1.38 As with the UTSA before it, and to a lesser extent the TRIPS Agreement, Article 3(4) of the Directive includes a provision that is designed to impose liability on third parties that may come to possess trade secrets that were first misappropriated by others. It provides that the acquisition, use or disclosure of the trade secrets of another 'shall also be considered unlawful whenever a person, at the time of the acquisition, use or disclosure, knew or should, under the circumstances, have known that the trade secret was obtained directly or indirectly from another person who was using or disclosing the trade secret unlawfully within the meaning of [Article 3(3)]'. As so written, it is consistent with the third party provisions of the UTSA. An important question under the

18 Council of the European Union, 9870/14, p. 4.

UTSA and the Directive is whether the third party must have knowledge of both the existence of a trade secret and of the misappropriation, or if knowledge of the misappropriation alone is enough. Also, the degree of knowledge is not specified, meaning that as a practical matter, the outcome of the case will come down to an equitable judgment.

A1.39 Paragraph (18) of the Preamble notes that although a third party may be held liable for trade secret misappropriation if he had the requisite knowledge, in situations where the original acquisition was in good faith, consideration should be given to alternatives to corrective measures and injunctions. Specifically, it provides: 'Member States should provide for the possibility, in appropriate cases, of pecuniary compensation being awarded to the injured party as an alternative measure, provided that such compensation does not exceed the amount of royalties or fees which would have been due had that person obtained authorization to use the trade secret in question'. This is similar to the discretionary 'royalty injunction' provision of US law, section 2(b) of the UTSA.

A1.40 Unlike the UTSA (section 1(2)(C)), the Directive does not contain a specific provision concerning trade secrets that are acquired by accident or mistake. However, the knowledge provision of Article 3(4) can be used to impose liability on a third party who acquires trade secrets by accident or mistake if the trade secret owner acts quickly to impose the requisite knowledge before any disclosure or use.

A1.41 An important question under both the Directive and the UTSA is whether the alleged misappropriator must know of the existence of trade secrets at the time of the misappropriation. Under both the Directive and US law, the answer to this question appears to be 'yes', particularly given the provisions regarding the imposition of liability on third parties and the reasonable efforts (or steps) requirement of the definition of a trade secret. As mentioned in Chapter 3, one of the central purposes of the reasonable efforts requirement of US trade secret law is to put others on notice of the existence of trade secrets (or at least the claim of trade secret protection), particularly given the lack of registration of trade secret rights. This is particularly important where there is no requirement that trade secrets exist in a tangible form.

D. Defences to trade secret misappropriation

A1.42 Unlike the UTSA which expresses several important limits on trade secret misappropriation in its commentary rather than its text, the Directive includes a provision (Article 4) that spells out the 'lawful acquisition, use and disclosure of trade secrets and exceptions'. Consistent with the commentary to the UTSA,

this includes the lawful activities of independent discovery or creation (Article 4.1(a)) and reverse engineering (Article 4.1(b)). It also includes a broad catch-all for actions consistent with honest commercial practices (Article 4.1(c)).

A1.43 Significantly, paragraph (10) of the Preamble to the Directive explains:

> In the interest of innovation and to foster competition, the provisions of this Directive should not create exclusive right on the know-how or information protected as trade secrets. Thus, independent discovery of the same know-how and information remains. Reverse engineering of lawfully acquired product is a lawful means of acquiring information except when otherwise agreed by contract. The freedom of entering into such contractual arrangements may however be limited by law, such as it is in the case of Article 5(3) of Directive 2009/24/EC of the European Parliament and the Council.

Unlike the UTSA, the Directive is explicit in suggesting that the right to conduct reverse engineering can be modified by contract, while also stating that the practice might be prohibited by law. Thus, the Directive does not resolve the thorny issue, extant in the United States as well, of whether the right of reverse engineering reflects strong public policy that should not be overwritten by contract. Article 5(3) of the Directive on the Protection of Computer Programs (referenced in the foregoing quote) is explicit in allowing reverse engineering of computer programs for limited purposes.

A1.44 Importantly, Article 4.1a of the Directive (added at the EU Council level and not to be confused with Article 4(1)(a) of the Directive) goes beyond the commentary to the UTSA to list an additional circumstance where the acquisition, use or disclosure of trade secrets is not actionable. It states that acquisition, use or disclosure of trade secrets is lawful 'to the extent that it is required or allowed by Union or national law'. This is a broad exception that has no explicit analogue in the UTSA. The EU is apparently trying to avoid what some governmental entities in the United States have not been able to avoid, namely, the assertion of trade secret rights by businesses with respect to information that governmental officials need to perform their functions. This relates to the issue of lack of transparency by regulated companies that is discussed in Chapter 6 and which is the topic of developing scholarship and case decisions within the United States.

A1.45 To provide substance and meaning to Article 4.1a, paragraph (10)(a) of the Preamble gives three specific, but not exclusive, examples of permissible activities. First, it notes that the exception is designed to allow administrative and judicial authorities to perform their duties. It specifically includes 'disclosure by Union institutions and bodies or national public authorities of business-related

information they hold pursuant to the obligations of Regulation (EC) No. 1049/2001 of the European Parliament and of the Council or to other rules on the public access to documents or on the transparency obligations of national public authorities', essentially the Freedom of Information Acts of EU countries. Thus, this provision sets up the same tension between open government laws and trade secret protection that exists in the United States (discussed in Chapter 6).

A1.46 The second exception discussed in paragraph (10)(a) of the Preamble concerns 'the acquisition and disclosure (not use) of trade secrets in the context of the exercise of the rights of workers representative to information, consultation and participation in accordance with Union and national law or practices'. There is no similar analogue in the UTSA, but the right of workers representatives to see confidential information of a business may be part of a collective bargaining agreement and be required under US labour law. Paragraph (10)(a) also contains an important limitation on the described right of workers representatives to acquire and disclose trade secrets, because such right is 'without prejudice of any duty of confidentiality imposed on the recipients of information so acquired'. Thus, the further use or disclosure of the information can be restricted.

A1.47 The third and final exception discussed in paragraph (10)(a) concerns the acquisition and disclosure (not use) of trade secret information in the context of 'statutory audits performed in accordance with Union or national law'. Again, there is no similar exception in the UTSA, but governmental entities in the United States routinely request information from companies in connection with audits. Generally, in the United States, in order to obtain the voluntary cooperation of businesses for the disclosure of information needed for an audit and other oversight, the applicable law, regulation or government contract will require that the information to be kept secret. Also, there are laws in the United States that make the disclosure of such information by governmental officials a crime.[19]

A1.48 Article 4.2 defines four additional 'lawful' activities related to the acquisition, use or disclosure of trade secrets. In very forceful language, it requires EU Member States to ensure that trade secret misappropriation claims are dismissed if the acquisition, use or disclosure of the trade secrets were:

(a) for making legitimate use of the right to freedom of expression and information;

19 See e.g., 41 USC s. 423 and 18 USC s. 1905.

(b) for the purpose of revealing an applicant's misconduct, wrongdoing or illegal activity, provided that the alleged acquisition, use or disclosure of the trade secret was necessary for such revelation and that the respondent acted in the public interest;
(c) the trade secret was disclosed by workers to their representatives as part of the legitimate exercise of their representative functions, provided that such disclosure was necessary for that exercise;
[(d) deleted by EU council];
(e) for the purpose of protecting a legitimate interest.

Although some case law exists within the United States to support some of these exceptions, particularly with respect to free speech issues and the public interest,[20] it is significant that the Directive explicitly spells them out in general terms. This will allow EU Member States flexibility to define such terms and further limit the scope of potential liability for trade secret misappropriation. With respect to the free speech exception, paragraph (10)(b) of the Preamble explains: 'Media often make public data or information considered to be a trade secret by another party but the publication of which could be in the public interest'.

A1.49 Article 7 of the Directive (as amended by the Council) does not establish a limitations period for trade secret misappropriation claims, leaving that issue to the discretion of each EU Member State. It states that each EU Member State has flexibility to determine 'when the limitations begin to run, the duration of the limitation period and the circumstances under which the limitation period is interrupted and suspended'. However, Article 7 also states that the limitation period must not exceed six years. This is a significant departure from the language of the UTSA (section 6) which sets a three-year statute of limitations and recognizes that trade secret misappropriation is not a continuing wrong. However, it remains to be seen which limitations period is selected by each EU Member State.

E. Availability of remedies, including the measure of damages

A1.50 Chapter III of the Directive generally defines the 'measures, procedures and remedies' that each EU Member State must provide for the enforcement of trade secret rights, specifically stating that 'civil redress' shall be available. Section 2 of Chapter III, starting with Article 9, concerns the available

20 See Pamela Samuelson, 'First Amendment Defenses in Trade Secrecy Cases' in Rochelle C. Dreyfuss and Katherine J. Strandburg (eds), *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research* (2011), p. 537.

remedies, starting with 'provisional and precautionary measures'. According to Article 9, the judicial authorities must have the ability to: (a) prohibit the use or disclosure of trade secrets on an interim basis; (b) prohibit the production or sale and importation of infringing goods; and (c) order the seizure or delivery up of suspected infringing goods, including imported goods. This is consistent with available preliminary injunctive relief under US law, but the nature of the available relief is specified in more detail in the Directive than in the UTSA.

A1.51 Paragraph (11) of the Preamble explains that: 'In line with the principle of proportionality the measures and remedies intended to protect trade secrets should be tailored to meet the objective of a smooth functioning internal market for research and innovation without jeopardizing other objectives and principles of public interest'. In addition to considering the interests of the trade secret owner, it specifically provides that judicial authorities should consider the interests of the defendant, third parties and consumers. There is no similar statement in the UTSA, although there is some language to this effect in both the commentary to the UTSA and its drafting history.

A1.52 Article 10 of the Directive, labelled 'Condition of application and safeguards' specifies the standards for the grant of preliminary relief in language that is similar to the US standards. First, Article 10(1) makes it clear that sufficient evidence must be presented on the issue of trade secret misappropriation. This is consistent with the US requirement that a trade secret owner must prove 'a likelihood of success on the merits' before obtaining preliminary relief. Also, Article 10(2), requires the competent judicial authorities to 'take into account the specific circumstances of the case', including such factors as the value of the alleged trade secrets, the steps taken to protect those secrets, and the conduct of the defendant in acquiring, using or disclosing the secrets. Consistent with US law concerning the grant of preliminary relief, the interests of third parties and the public must also be considered.

A1.53 The remaining provisions of Article 10 can best be described as limitations on the grant of preliminary relief in trade secret cases (at least to the extent that the provisions are not already a part of an EU Member State's laws). First, Article 10(3) specifies that preliminary relief must be revoked unless a case leading to a decision on the merits is instituted in a timely fashion or in the event that the subject information no longer meets the definition of a trade secret 'for reasons that cannot be attributed to the respondent'. Article 10(4) is an optional provision which states that the grant of preliminary relief may be conditioned on 'the lodging by the applicant of adequate security'. Finally, in the event that preliminary relief is revoked pursuant to Article 3(a), Article 10(5) requires EU Member States 'upon the request of respondent or of an injured third party, to

provide the respondent or the injured third party, appropriate compensation for any injury caused thereby'. As described in Chapters 3 and 6, all of the foregoing concepts exist in US law except that ordinarily third parties are not allowed to seek compensation related to the issuance of an improper preliminary injunction (only parties).

A1.54 As in the United States, whether preliminary relief will be granted depends in large part on the procedural rules and equitable principles of each EU Member State. As a practical matter, it also depends upon how quickly a request for preliminary relief is scheduled for a hearing. Nothing in the text of the Directive or the UTSA requires prompt action, except that Article 5(2)(b) of the Directive provides that the available civil redress should 'not be unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays'. Further, paragraph (15) of the Preamble stresses the importance of 'fast effective and accessible provisional measures … without having to await a decision on the substance of the case'.

A1.55 Chapter III, Section 3 of the Directive concerns remedies following a decision on the merits of a case and mirrors the remedies that are specified in sections 2 through 4 of the UTSA. Article 11 of the Directive concerns injunctive relief and corrective measures following a decision on the merits and is generally more detailed than the corresponding provision of the UTSA (section 2). It provides that the judicial authorities may: (a) prohibit the use or disclosure of trade secrets; (b) prohibit the production, sale or importation of infringing goods; and (c) adopt corrective measures with respect to infringing goods. US courts have similar powers, but what is different about the Directive as compared to the UTSA is its explicit recognition of the possibility of 'infringing goods' and its definition of that term.

A1.56 As discussed previously, according to Article 2(4) of the Directive, 'infringing goods' means 'goods whose design, quality, manufacturing process or marketing significantly benefits from trade secrets unlawfully acquired, used or disclosed'. Thus, there is explicit recognition of the fact that injunctions will not be issued to prevent the production and sale of goods containing trade secrets unless the trade secrets are a significant part of the goods. However, unlike the UTSA, the Directive explicitly recognizes that the seizure or destruction of infringing goods may be necessary at times, thereby shifting the focus from trade secrets per se to goods that are the product of the use of trade secrets or in which trade secrets are embedded.

A1.57 Assuming that the goods in question meet the definition of infringing goods, Article 11(2) of the Directive provides the following non-exclusive list of

corrective measures that can be ordered with respect to such goods: recalling the goods from the market; depriving the goods of their infringing quality; destruction of the infringing goods; and destruction or delivering up of the documents containing the trade secrets. Article 11(3) and (4) specify certain particulars with respect to the grant of the foregoing remedies. Generally, the types of measures that are set forth in Article 11 are similar to permanent injunction orders that have been granted in the United States, but pursuant to the broad discretionary powers of the court rather than based upon details in the UTSA or its commentary.

A1.58 Article 12 is directly related to Article 11 in that it specifies the conditions for granting injunctive relief and corrective measures and related safeguards. As discussed in Chapter 6, because injunctive relief is a form of equitable relief, courts in the United States generally consider 'the equities' before granting permanent injunctive relief. Article 12(1) of the Directive is similar to US law in this regard, but unlike the UTSA, it specifically lists a number of factors to be considered, including: the value of the trade secrets; the measures taken to protect the trade secret; the conduct of the infringer; the impact of the wrongdoing; the legitimate interests of the parties and third parties; and the public interest.

A1.59 Similar to the language of the UTSA (section 2), the last part of Article 12(1) and the entirety of Article 12(2) combine to limit the length of permanent injunctive relief. It should at least be long enough to 'eliminate any commercial or economic advantage' derived from the misappropriation and should end when the trade secret ceases to exist due to no fault of the infringer. This is similar to the 'lead-time advantage' injunction concept under US law. Paragraph (16) of the Preamble provides that 'no measure of this type should be enforceable if the information originally covered by the trade secret is in the public domain for reasons that cannot be attributed to the respondent'. This is also consistent with US law.

A1.60 Like section 2(b) of the UTSA, Article 12(3) of the Directive provides that judicial authorities shall have the authority to order pecuniary compensation (measured by reasonable royalties) in lieu of an injunction (a so-called 'royalty injunction'). However, three specified conditions must be met which, although similar conceptually to the 'exceptional circumstances' of US law, appear to provide a more limited exception: first, as under US law, the option of reasonable royalties in lieu of an injunction is principally for individuals and companies who do not have the requisite knowledge 'at the time of use or disclosure'; second, the grant of an injunction would cause the person or

company 'disproportionate harm'; third, pecuniary compensation must be 'reasonably satisfactory'. As in the US, the first requirement should apply to trade secrets that were acquired by accident or mistake.

A1.61 The available measure of damages for trade secret misappropriation is specified in Article 13 of the Directive and reflects a broad conception of possible damages consistent with section 3 of the UTSA. In addition to damages measured by 'actual prejudice suffered', the Directive states that factors such as the 'unfair profits made by the infringer' and 'elements other than economic factors' should be considered. Similar to section 3(a) of the UTSA, 'in appropriate cases' Article 13(2) of the Directive also states that judicial authorities should be allowed to set the amount of damages based upon 'royalties or fees which would have been due if the infringer had requested authorization'.

A1.62 What is unique about Article 13 of the Directive compared to US law is the second paragraph of Article 13(1) which states: 'In accordance with their national law and practice, Member States may restrict the liability for damages to employees toward their employers … when they act without intent'. This appears to be part of a compromise as the original draft Directive included an intent requirement that was modified by the EU Council. However, it also reflects an overarching concern, reflected in other explicit limitations, about the effect of trade secret misappropriation on employee mobility, a fundamental right under EU law.[21] On the other hand, Article 13 calls for remedies to be awarded for 'moral prejudice' (or non-economic harm), a concept that is not included in the UTSA or generally recognized under US commercial law.

A1.63 Article 14 of the Directive concerns the publicity of trade secret cases and the potential publication of judicial decisions in such cases and, in so doing, reflects the very real possibility that the laws of a country, including its judicial decisions, may not be as accessible as they are in the United States. It also reflects the potential value of publicizing case decisions. Paragraph (20) of the Preamble explains: 'To act as a supplementary deterrent to future infringers and to contribute to the awareness of the public at large, it is useful to publicise decisions, including where appropriate through prominent advertising'.

A1.64 Article 14(1) provides that EU Member States shall ensure that a prevailing trade secret owner may request a court order to require the dissemination of information about the case at the expense of the infringer. Article 14(2) states that such publicity shall preserve the confidentiality of the trade secrets. Article 14(3) is a litany of factors that the judicial authorities should consider in

21 Council of the European Union, 9870/14.19, Preamble, para. (23).

deciding whether to grant a request to publish the judicial decision. No similar provisions exist in the UTSA or elsewhere in US law; however, the grant of such an order would normally be within the discretion of US courts.

A1.65 Article 15 of the Directive is an important corollary to the power of judicial authorities to grant injunctive relief and make other orders. It requires EU Member States to 'ensure that the competent judicial authorities may impose sanctions' on persons who fail to comply with specified orders. US courts already have such power and, in fact, can fine and imprison those who are held in contempt of court orders following a hearing on the issue.

A1.66 Unlike the UTSA, no provision of the Directive addresses the award of punitive damages (section 3(b) of the UTSA) or attorney's fees (section 4 of the UTSA), but this does not necessarily mean that such relief is unavailable in EU countries. Rather, other provisions of the laws of EU countries should be consulted to determine whether and under what circumstances punitive damages and the award of attorney's fees are available. In this regard, paragraph (19) of the Preamble states: 'The aim is not to introduce an obligation to provide for punitive damages, but to ensure compensation based upon an objective criterion while taking account of the expenses incurred by the holder of the trade secret'.

F. Protecting trade secrets during litigation

A1.67 Article 8 of the Directive is the provision that requires EU Member States to ensure that trade secrets will be protected during applicable legal proceedings and is similar to section 5 of the UTSA. Specifically, Article 8(1) requires EU Member States to ensure that the individuals who are involved in such proceedings 'shall not be permitted to use or disclose any trade secret or alleged trade secret of which they have become aware as a result of such participation or access'. Unlike the UTSA, Article 8(2) does not specifically refer to the US procedural device known as a 'protective order', but rather to 'specific measures' that judicial authorities may take to protect trade secrets, including restricting access to documents that contain trade secrets and restricting access to hearings.

A1.68 The subdivisions of Article 8(1) make it clear that the obligation to protect trade secrets in the course of legal proceedings does not apply to information that is found not to meet the requirements for trade secret protection and information which, over time, has lost its trade secret status. This is consistent with the law in the United States, although not the express language of section 5 of the UTSA. Also, pursuant to Article 8(3), in deciding whether to undertake measures to protect the confidentiality of trade secrets during or after applicable

legal proceedings, the judicial authorities must consider a number of factors, including the need to ensure a fair trial and the needs of the parties and third parties.

G. Public policy limits on scope and application of trade secret protection

A1.69 In contrast to US law, where the public policy limits on the scope and application of trade secret law are often expressed in case law or in the commentary to the UTSA, the Directive contains explicit textual references to limits and safeguards. In addition to the limitations and exceptions discussed below, Article 5(2) requires that the measures, procedures and remedies that each country must provide must: (a) be fair and equitable; (b) not be unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays; and (c) be effective and dissuasive. This is consistent with the general principles and goals of the US justice system and the requirements of the TRIPS Agreement.

A1.70 Article 6 of the Directive also differs from the UTSA in its explicit textual reference to the need for 'proportionality' and the need to avoid abuses in litigation, although it is similar to the UTSA in allowing judicial authorities to impose 'appropriate measures' if trade secret misappropriation claims are brought or pursued in bad faith. (Compare Article 6(1) with Article 6(2).) The measures that can be imposed include 'awarding damages to the respondent, imposing sanctions on the applicant or ordering the dissemination of the information concerning the decision taken in accordance with Article 14'. Arguably, courts in the United States have the power to impose similar measures against abusive litigation but they are often reticent to do so and the UTSA only specifically allows for the grant of attorney's fees (see section 4).[22]

A1.71 An important part of Article 6 is the statement in Article 6(1)(b) that trade secret protection measures should be designed to avoid 'the creation of barriers to legitimate trade in the internal market'. Noting the potential anticompetitive effects of abusive trade secret litigation, paragraph (12) of the Preamble states: 'The smooth functioning of the internal market would be undermined if the measures and remedies provided for were used to pursue illegitimate intents incompatible with the objectives of the Directive'.

22 See generally Elizabeth A. Rowe, 'Trade Secret Litigation and Free Speech: Is it Time to Restrain the Plaintiffs?' (2009) 50 *BCL Rev.* 1425.

A1.72 As previously discussed in Chapter 2, the assertion of intellectual property rights in anticompetitive ways was a major concern of many of the participants in the NG11 negotiations that resulted in the TRIPS Agreement and found voice in Article 8.2 of that Agreement. Including this concept in a specific provision of the Directive goes a step further by explicitly tying a general concern to a specific set of laws. Additionally, section 2 of the Explanatory Memorandum recognizes these concerns when it states that 'competition should not be restricted as no exclusive rights are being granted and … the hiring and mobility of highly skilled labour (those who have access to trade secrets) within the Internal Market should not be negatively impacted'.

A1.73 The words 'proportionality' or 'proportionate' are used in several places in the Directive, with different apparent meanings. As used in Article 6(1)(a), the word 'proportionate' appears to refer to the principle of proportionality that is set forth in Article 5 of the Treaty on the European Union. It states: 'Under the principle of proportionality, the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties'. This means that the Directive is limited in its coverage and that the non-trade secret laws and legal principles of EU Member States will continue to develop as before. This is generally the case in the United States when one considers the potential overlap between trade secret law and separate laws governing restraints of trade and employment issues, including employee mobility and the enforceability of non-compete agreements (discussed in Chapter 5). In practice, however, these different bodies of law can give rise to conflicts that judicial officials must resolve in trade secret cases. In the same way that the different US states have different ways of dealing with these issues, trade secret owners should anticipate that the different countries of the EU will have different approaches.

A1.74 Paragraph (10)(c) of the Preamble (added by the EU Council) speaks directly to 'collective agreements' between 'social partners', presumably including the sorts of business-to-business relationships that are described in Chapter 4 and the employer/employee relationships described in Chapter 5. Specifically, it states that the Directive should not affect agreements concerning 'duties not to disclose a trade secret or to limit its use and the consequences of a breach of such duties by the party subject to them, provided that any such collective agreement does not restrict the safeguards'. Thus, the pre-existing laws of each EU Member State with respect to such agreements will continue to apply but with the safeguards of the Directive being applied to limit those agreements as necessary.

A1.75 Given the EU's proportionality principle and statements throughout the European Commission Study and the proposed Directive which note the need for

limits on the scope of trade secret protection, attorneys who advise clients with respect to the protection of trade secrets in EU Member States (either before or after the implementation of the EU Trade Secret Directive) should be careful to point out the potential applicability of other legal principles which may limit the scope of available trade secret protection. In other words, the non-trade secret laws of individual countries may apply and the Trade Secret Directive and such other laws must be read through the lens of applicable EU law.

APPENDIX 2: PROPOSAL FOR A DIRECTIVE OF THE EUROPEAN PARLIAMENT ON TRADE SECRETS

Proposal for a Directive of the European Parliament on Trade Secrets, with interlineations and strike-outs added to reflect changes made to the draft text at the 14 May 2014 meeting of the Permanent Representative Committee of the Council of the European Union, comparing Docs. 9475/14 and 9870/14.*

EXPLANATORY MEMORANDUM

I. CONTEXT OF THE PROPOSAL

Europe is strong on science and innovation and it has the potential to become a global leader. Striving for science quality is not just the aim of researchers, but provides important public and private returns. Nevertheless, overall research and development (R&D) within the EU is not sufficiently driven by businesses when compared to some major trading partners, in particular the US and Japan. Sub-optimal business investment in R&D adversely impacts on the introduction of new products, processes, services and know-how. **A2.01**

It is therefore desirable to improve the conditions for innovative business activity. As part of its wider Europe 2020 strategy, the Commission has undertaken to create an Innovation Union, protecting investments in the **A2.02**

* The page numbering in this document is not consistent with the original documents and due to the interlineations, the footnote numbering is also not the same as in the original documents. The language that is struck out was deleted by the Council. The language in bold and italic was added by the Council.

knowledge base, reducing costly fragmentation, and making Europe a more rewarding place for innovation. An environment conducive to innovation should in particular encourage higher levels of investment in R&D by the private sector, through more extensive, including cross-border, collaboration in R&D and technological developments between universities and industry, open innovation and allowing for improved valuation of intellectual property (IP) such that access to venture capital and financing is enhanced for research-oriented and innovative economic agents. Attaining such goals exclusively on a national level is not sufficient and would lead to inefficient duplication of effort in the Union.

A2.03 The drastically reduced transaction costs in the digital economy have led to new forms of cooperation with open science and open innovation, often leading to new business models for using co-created knowledge. Nevertheless, intellectual property rights (IPRs) are an essential part of an innovation policy. IPRs provide innovators and creators with means of appropriation of the outputs of their efforts, which are intangible in nature, thus providing the necessary incentives for investment in new solutions, inventions and know-how. IPRs tend to protect the results of creative or inventive efforts, but they have a limited scope of application.

During the process of research and creation significant information is compiled and developed, progressively building knowledge of a substantial economic value that often does not qualify for IPR protection, but which is equally important for innovation and for the competitiveness of businesses in general. When securing such assets and attracting financing and investment requires IP to be kept secret, companies, laboratories, universities, as well as the individual inventors and creators, use the most relied upon and long-standing form of appropriation over valuable information: confidentiality.

A2.04 As research builds on prior work, sharing of knowledge and new findings represent important leverage for further innovation. Depending on the business model of the innovator there are cases when confidentiality may be the requisite basis upon which IP can be nurtured in order for it to be exploited into innovation and increased competitiveness. Every IPR starts with a secret. Writers do not disclose the plot they are working on (a future copyright), car makers do not circulate the first sketches of a new model (a future design), companies do not reveal the preliminary results of their technological experiments (a future patent), companies hold on to the information relating to the launch of a new branded product (a future trade mark), etc.

A2.05 In legal terminology, information that is kept confidential in order to preserve competitive gains is referred to as 'trade secrets', 'undisclosed information', 'business confidential information' or 'secret know-how'. Business and academia sometimes use other name tags for it such as 'proprietary know-how' or 'proprietary technology'.

A2.06 Trade secrets are also just as important in protecting non-technological innovation. The services sectors, representing some 70% of EU GDP, are very dynamic, and that dynamism depends on innovative knowledge creation. However, the services sector does not rely as much as manufacturing industry on technological process and product innovation (as protected by patents). Confidentiality in this key part of the EU economy is used to build and exploit so-called 'soft' innovation for competitiveness, covering the use and application of a diversified range of strategic commercial information, which extends beyond technological knowledge, such as information on customers and suppliers, business processes, business plans, market research, etc.

A2.07 Economists agree that companies, irrespective of their size, value trade secrets at least as much as all other forms of IP. Trade secrets are particularly important to small- and medium-sized enterprises (SMEs) and start-ups as these often lack specialised human resources and financial strength to pursue, manage, enforce and defend IPRs.

A2.08 Although not protected as a classical IPR, trade secrets are nevertheless a key complementary instrument for the required appropriation of intellectual assets that are the drivers of the knowledge economy of the 21st century. The holder of a trade secret does not have exclusive rights over the information covered by the trade secret. However, in order to promote an economically efficient and competitive process, restrictions to the use of the trade secret are justified in cases where the relevant know-how or information has been obtained from the trade secret holder against its will by a third party through dishonest means. The assessment of whether and to what extent such restrictions are necessary is subject, on a case-by-case basis, to judicial control.

A2.09 This means that competitors are free, and should be encouraged, to develop and use the same, similar or alternative solutions, thus competing in innovation, but are not allowed to cheat, steal or deceive in order to obtain confidential information developed by others.

A2.10 While the development and management of knowledge and information have become ever more central to the performance of the EU economy, the exposure of valuable undisclosed know-how and information (trade secrets) to theft,

espionage or other misappropriation techniques has and continues to increase (globalisation, outsourcing, longer supply chains, increased use of ICT, etc.). The risk also increases that stolen trade secrets are used in third countries to produce infringing goods which subsequently compete within the EU with those of the victim of the misappropriation. However, the current diversity and fragmentation of the legal framework on the protection of trade secrets against their unlawful acquisition, use or disclosure is impairing cross-border R&D and the circulation of innovative knowledge by undermining the capacity of European companies to respond to dishonest attacks on their know-how.

A2.11 Optimisation of the IP infrastructure is one important pillar of the Innovation Union and, in that context, the Commission adopted in May 2011 a comprehensive IP strategy, undertaking to examine the protection of trade secrets.[1] This proposal is one further deliverable on the commitment of creating a single market for intellectual property.

II. RESULTS OF CONSULTATIONS WITH THE INTERESTED PARTIES AND IMPACT ASSESSMENTS

A. Public consultation

A2.12 This initiative is based on an evaluation of the importance of trade secrets for innovation and for the competitiveness of companies, the extent to which they are used, their role, and relationship with IPRs, in the generation and economic exploitation of knowledge and intangibles assets, and the relevant legal framework. These assessments were carried out with the help of two external studies and with extensive consultations of stakeholders.

A2.13 A first study (published in January 2012) provides a comparative law assessment of the protection against misappropriation of trade secrets in the different EU Member States. A second study, published in May 2013, assessed the economic foundations of trade secrets and protection against their misappropriation and further analysed the legal protection of trade secrets throughout the EU. It confirmed the fragmented and diversified nature of the existing protection against misappropriation of trade secrets throughout the Union, considering it to be, in general, opaque and imposing unnecessary costs and risks. The study considered that an efficient system to secure the results of R&D is a precondition for businesses to innovate and that the flexibility offered by efficient reliance on trade secrets fits well with the way in which innovation takes place in

1 COM(2011)287.

today's business environment. It concluded that harmonisation of trade secret law in the EU would improve conditions for firms to develop, exchange and use innovative knowledge.

A2.14 The views of stakeholders were collected in 3 steps. First, civil society, industry, academia and public authorities discussed this issue in a conference organised by the Commission that took place in June 2012.

A2.15 Second, a survey on trade secret use, associated risks and legal protection was subsequently launched, in the context of the 2nd study, in November 2012. The survey was directed to a representative sample of businesses across the EU, including SMEs which accounted for 60% of the sample. A total of 537 responses to the survey were received. Overall, 75% of respondents ranked trade secrets as strategically important to their company's growth, competitiveness and innovative performance. The survey revealed that over the last 10 years, about one in five respondents had suffered at least one attempt at misappropriation within the EU, whereas nearly two in five respondents stated that the risk of trade secret misappropriation had increased during the same period. Two in three of the respondents indicated support for an EU legislative proposal.

A2.16 Third, from 11 December 2012 until 8 March 2013 the services of the Commission carried out an open public consultation, focusing on the possible policy options and their impacts. 386 replies were received, mostly from individual citizens (primarily from one Member State) and businesses. 202 respondents found that the legal protection against the misappropriation of trade secrets should be addressed by the EU. However, the views expressed by the two main groups of respondents (citizens and companies) were polarised. Three in four citizens regard trade secrets as having low importance for R&D and find existing legal protection of trade secrets excessive and 75% do not see a need for an EU action. Responding companies, on the other hand, consider trade secrets as highly important for R&D and for their competitiveness. A significant majority regard existing protection as weak, in particular at the cross-border level, and see differences between national legal frameworks as having negative impacts such as higher business risk in the Member States with weaker protection, less incentive to undertake cross-border R&D and increased expenditure in preventive measures to protect information.

B. Impact assessment

A2.17 The impact assessment showed the national divergences in the protection of trade secrets: few Member States' laws either define trade secrets or specify when they should be protected; cease and desist orders against infringers are not

available in all cases; traditional rules on the calculation of damages are often inadequate for trade secret misappropriation cases and alternative methods (e.g. amount of royalties that would have been due under a licence agreement) are not available in all Member States; and criminal rules do not address trade secret theft in all Member States. In addition, many Member States do not have rules aimed at safeguarding trade secrets during litigation, thus deterring victims of trade secret misappropriation from seeking redress in court.

A2.18 Two main problems resulted:

- Sub-optimal incentives for cross-border innovation activities. When trade secrets are under a risk of misappropriation with ineffective legal protection, incentives to undertake innovation activities (including at cross-border scale) are affected because of (i) the lower expected value of innovation relying on trade secrets and the higher costs for protecting it; and (ii) the higher business risk when sharing trade secrets. For instance, 40% of EU companies would refrain from sharing trade secrets with other parties because of fear of losing the confidentiality of the information through misuse or release without their authorisation. This inhibits innovation and in particular collaborative research and open innovation which requires sharing of valuable information by multiple business and research partners.
- Trade secret-based competitive advantages are at risk (reduced competitiveness): the fragmented legal protection within the EU does not guarantee a comparable scope of protection and level of redress within the Internal Market, thus putting trade-secret based competitive advantages, whether innovation-related or not, at risk and undermining trade secret owners' competitiveness. For instance, the European chemical industry, which strongly relies on process innovation secured by trade secrets, estimates that misappropriation of a trade secret could often entail a turnover reduction of up to 30%.

A2.19 The objective of the initiative is to ensure that the competitiveness of European businesses and research bodies which is based on undisclosed know-how and business information (trade secrets) is adequately protected and improve the conditions/framework for the development and exploitation of innovation and for knowledge transfer within the Internal Market. Specifically, it aims at improving the effectiveness of the legal protection of trade secrets against misappropriation throughout the Internal Market.

A2.20 The following possible options for resolving the problem were considered:

- Status quo.
- Provide information on and raise awareness of the national measures, procedures and remedies available against trade secret misappropriation.
- Convergence of national civil law as regards the unlawfulness of acts of misappropriation of trade secrets (but rules on remedies and preservation on confidentiality of trade secrets during legal proceedings to be decided at national level).
- Convergence of national civil law remedies against the misappropriation of trade secrets and rules on preservation of confidentiality of trade secrets during and after legal proceedings (in addition to option 3).
- Convergence of national criminal law in addition to civil law convergence (option 4), including rules on minimum criminal penalties.

A2.21 The impact assessment concluded that option 4 would be proportionate and would best serve to achieve the objectives pursued.

A2.22 In terms of impacts, the convergence of civil law remedies would allow innovative businesses to defend their rightful trade secrets more effectively across the EU. Also, if trade secrets owners could rely on confidentiality during proceedings, they would be more inclined to seek legal protection against potential damages through misappropriation of trade secrets. Increased legal certainty and convergence of laws would contribute to increasing the value of innovations companies try to protect as trade secrets, as the risk of misappropriation would be reduced. Positive impacts on the functioning of the Internal Market result as companies, in particular SMEs, and researchers will be able to make better use of their innovative ideas by cooperating with the best partners across the EU, thus helping to increase private sector investment in R&D within the Internal Market. At the same time, competition should not be restricted as no exclusive rights are being granted and any competitor is free to independently acquire the knowledge protected by the trade secret (including by reverse engineering).

A2.23 Similarly, the hiring and mobility of highly skilled labour (those who have access to trade secrets) within the Internal Market should not be negatively impacted. This should have, over time, positive effects on the competitiveness and growth of the EU economy. This initiative does not negatively affect fundamental rights. In particular, the initiative will promote the right to property and the right to conduct a business. In terms of access to documents in judicial proceedings safeguards have been put in place in order to safeguard the right of defence. The initiative also contains safeguards to ensure that the right to freedom of expression and information is guaranteed.

A2.24 This initiative is consistent with international obligations (i.e. the Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS Agreement)). Major trading partners have similar legislation on this issue.

C. Legal elements of the proposal

A2.25 Article 114 of the Treaty on the Functioning of the European Union (TFEU) provides for the adoption of EU rules harmonising national legislation, whenever necessary for the smooth functioning of the Internal Market. The objective of the proposal is to establish a sufficient and comparable level of redress across the Internal Market in case of trade secret misappropriation (while providing sufficient safeguards to prevent abusive behaviour). The existing national rules offer an uneven level of protection across the EU of trade secrets against misappropriation, which jeopardises the smooth functioning of the Internal Market for information and know-how. Indeed, in order to fulfil all its potential as an economic asset, valuable information (such as manufacturing processes, new substances and materials, non-patented technology, business solutions) must be transferable, in confidence, as it may have different uses for different players in different geographic regions, thus generating income for creators and allowing for an efficient allocation of resources. The scattered legal framework also reduces the incentives to undertake any innovation-related cross-border activity which would depend on the use of information protected as a trade secret, such as establishment in a different Member States for the purposes of manufacturing or marketing goods/services based on trade secrets, supplying goods/services to a company in other Member State or outsourcing the manufacturing to another company in a Member State. In those situations, if the trade secret is misappropriated in another country with lower levels of protection, infringing goods may spread across the market. Existing national rules thus render cross-border network R&D and innovation less attractive and more difficult. They also create a higher business risk in Member States with lower levels of protection, with adverse effects on the whole of the EU economy as, on the one hand, incentives to cross-border trade diminish, and on the other hand, 'infringing goods' originating from those Member States (or imported through them) may spread across the Internal Market. The proposal should facilitate cross-border R&D cooperation: a clear, sound and levelled protection of trade secrets against misappropriation promotes cross-border sharing and transfer of confidential business information and know-how by diminishing perceived risks and transactions costs associated with multiple legislation handling. It should also improve incentives to cross-border trade, thanks to the reduction of unfair competition from free-riders in the cross-border market space.

In terms of subsidiarity, the problems identified in the impact assessment are driven by the diversity and inconsistency of the existing regulatory framework that does not ensure a level playing field for EU companies with adverse consequences for their competitiveness and that of the EU as a whole. Achieving greater consistency in redress measures across Member States is central to addressing those problems. Yet such consistency cannot be achieved by action taken solely on the Member State level: experience in this field shows that even when Member States are coordinated to a certain extent, e.g. by the TRIPS Agreement, a sufficient degree of substantive harmonisation of national rules is not achieved. Hence, the necessary scale and effects of the proposed action are at EU level. **A2.26**

III. BUDGETARY IMPLICATION

The proposal has no impact on the European Union budget. All actions proposed to be taken up by the Commission in this proposal are consistent and compatible with the new Multiannual Financial Framework 2014–2020. **A2.27**

IV. EXPLANATION OF THE PROPOSAL

A. General provisions

Chapter I defines the subject matter (Article 1): the Directive applies to unlawful acquisition, disclosure and use of trade secrets and the measures, procedures and remedies that should be made available for the purpose of civil law redress. **A2.28**

Also in Chapter I, Article 2 defines key concepts. The definition of 'trade secret' contains three elements: (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. This definition follows the definition of 'undisclosed information' in the TRIPS Agreement. **A2.29**

The definition of 'trade secret holder' incorporates, also following the TRIPS Agreement, the concept of lawfulness of control of the trade secret as a key element. It therefore ensures that not only the original owner of the trade secret but also licensees can defend the trade secret. **A2.30**

A2.31 The definition of 'infringing good' integrates a proportionality assessment. The goods which are designed, manufactured or marketed carrying out an unlawful conduct must benefit to a significant degree from the trade secret in question to be considered as infringing goods. The test should be used when considering any measures directly affecting goods manufactured or put in the market by an infringer.

A2.32 Chapter II sets the circumstances under which the acquisition, use and disclosure of a trade secret is unlawful (Article 3), thus entitling the trade secret holder to seek the application of the measures and remedies foreseen in the Directive. The key element for those acts to be unlawful is the absence of consent of the trade secret holder. Article 3 also determines that the use of a trade secret by a third party not directly involved in the original unlawful acquisition, use or disclosure is also unlawful, whenever that third party was aware, should have been aware, or was given notice, of the original unlawful act. Article 4 expressly clarifies that independent discovery and reverse engineering are legitimate means of acquiring information.

B. Measures, procedures and remedies

A2.33 Chapter III establishes the measures, procedures and remedies that should be made available to the holder of a trade secret in case of unlawful acquisition, use or disclosure of that trade secret by a third party.

A2.34 Section 1 sets the general principles applicable to the civil enforcement instruments in order to prevent and repress acts of trade secret misappropriation, notably effectiveness, fairness and proportionality (Article 5) and safeguards to prevent abusive litigation (Article 6). Article 7 establishes a period of limitation. Article 8 requires that Member States provide judicial authorities with mechanisms to preserve the confidentiality of trade secrets disclosed in court for the purpose of litigation. The possible measures must include: restricting access to documents submitted by the parties or third parties, in whole or in part; restricting access to hearings and hearing records; ordering the parties or third parties to prepare non-confidential versions of documents containing trade secrets and also preparing non-confidential versions of judicial decisions. These measures should be applied in a proportionate manner so that the rights of the parties to a fair hearing are not undermined. The confidentiality measures must apply during litigation, but also after litigation in case of requests of public access to documents for as long as the information in question remains a trade secret.

Section 2 provides for provisional and precautionary measures in the form of interlocutory injunctions or precautionary seizure of infringing goods (Article 9). It also establishes safeguards to ensure the equity and proportionality of those provisional and precautionary measures (Article 10). **A2.35**

Section 3 provides for measures that may be ordered with the decision of the merits of the case. Article 11 provides for the prohibition of use or disclosure of the trade secret, the prohibition to make, offer, place on the market or use infringing goods (or import or store infringing goods for those purposes) and corrective measures. The corrective measures request, *inter alia*, the infringer to destroy or deliver to the original trade secret holder all the information he or she holds with regard to the unlawfully acquired, used or disclosed trade secret. Article 12 establishes safeguards to ensure equity and proportionality of the measures provided for in Article 11. **A2.36**

The awarding of damages for the prejudice suffered by the trade secret holder as a consequence of the unlawful acquisition, use or disclosure of his/her trade secret is enshrined in Article 13, which calls for the taking into consideration of all the relevant factors, including the unfair profits obtained by the defendant. The possibility of calculating the damages on the basis of hypothetical royalties is also made available, in line of what is foreseen in the case of infringements of intellectual property rights. **A2.37**

Article 14 empowers the competent judicial authorities to adopt publicity measures at the request of the plaintiff, including the publication of the decision on the merits of the case – provided that the trade secret is not disclosed and after considering the proportionality of the measure. **A2.38**

The Directive does not integrate rules on the cross-border enforcement of judicial decisions as general EU rules on this matter apply, allowing the enforcement in all Member States of a court judgment prohibiting the import into the EU of infringing goods. **A2.39**

C. Sanctions, reporting and final provisions

In order to ensure an effective application of the Directive and the fulfilment of the pursued objectives, *Chapter IV* foresees the application of sanctions in case of non-compliance with the measures provided for in Chapter III and comprises provisions on monitoring and reporting. **A2.40**

A2.41 The Commission considers that, in line with the joint declarations concerning explanatory documents,[2] there are not sufficient arguments to formally request explanatory documents from Member States to explain the relationship between the content of the Directive and the corresponding parts of national transposition instruments. From a technical perspective, the Directive is not particularly complex, contains only a limited number of legal obligations that require transposition into national law and deals with a well delimited issue that has already been regulated at national level as regards the neighbouring area of IPRs. Therefore, the transposition at national level is not expected to be complicated and this should ease the monitoring of such transposition.

2 OJ C369 of 17.12.2011, pp. 14–15.

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 2013/0402 (COD)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national Parliaments,

Having regard to the opinion of the European Economic and Social Committee,[3]

~~After consulting the European Data Protection Supervisor,~~[4]

Acting in accordance with the ordinary legislative procedure,[4]

Whereas:

(1) Businesses and non-commercial research institutions invest in acquiring, developing and applying know-how and information, which is the currency of the knowledge economy. This investment in generating and applying intellectual capital determines their competitiveness in the market and therefore their returns to investment, which is the underlying motivation for business research and development. Businesses have recourse to different means to appropriate the results of their innovative activities when openness does not allow for the full exploitation of their research and innovation investments. Use of formal intellectual property rights such as patents, design rights or copyright is one of them. Another is to protect access and exploit the knowledge that is valuable to the entity and not widely known. Such know-how and business information,

---

3 OJ C, p.

~~4 OJ C, p.~~

4 Position of the European Parliament of … (not yet published in the Official Journal) and decision of the Council of …

that is undisclosed and intended to remain confidential is referred to as a trade secret. Businesses, irrespective of their size, value trade secrets as much as patents and other forms of intellectual property right and use confidentiality as a business ***competitiveness*** and research innovation management tool, covering a diversified range of information, which extends beyond technological knowledge to commercial data such as information on customers and suppliers ***(which may involve personal data)***, business plans or market research and strategies. By protecting such a wide range of know-how and commercial information, whether as a complement or as an alternative to intellectual property rights, trade secrets allow the creator to derive profit from his/her creation and innovations and therefore are particularly important ***for business competitiveness as well as*** for research and development and innovative performance.

(2) Open innovation is an important lever for the creation of new knowledge and underpins the emergence of new and innovative business models based on the use of co-created knowledge. Trade secrets have an important role in protecting the exchange of knowledge between businesses ***and research institutions*** within and across the borders of the internal market in the context of research and development and innovation. Collaborative research, including cross-border cooperation, is particularly important to increase the levels of business research and development within the internal market. Open innovation is a catalyst for new ideas to find their way to the market meeting the needs of consumers and tackling societal challenges. In an internal market where barriers to such cross-border collaboration are minimised and where cooperation is not distorted, intellectual creation and innovation should encourage investment in innovative processes, services and products. Such an environment conducive to intellectual creation and innovation is also important for employment growth and improving competitiveness of the Union economy. Trade secrets are amongst the most used form of protection of intellectual creation and innovative know-how by businesses, yet they are at the same time the least protected by the existing Union legal framework against their unlawful acquisition, use or disclosure by ~~third~~ ***other*** parties.

(3) Innovative businesses are increasingly exposed to dishonest practices aiming at misappropriating trade secrets, such as theft, unauthorised copying, economic espionage, breach of confidentiality requirements, whether from within or from outside of the Union. Recent developments, such as globalisation, increased outsourcing, longer supply chains, increased use of information and communication technology, contribute to increasing the risk of those practices. The unlawful acquisition, use or disclosure of a trade secret compromises the legitimate trade secret holder's ability to obtain first mover returns using the

outputs of its innovative efforts. Without effective and comparable legal means for defending trade secrets across the Union, incentives to engage in innovative cross-border activity within the internal market are undermined and trade secrets are unable to fulfil their potential as drivers of economic growth and jobs. Thus, innovation and creativity are discouraged and investment diminishes, affecting the smooth functioning of the internal market and undermining its growth enhancing potential.

(4) International efforts taken in the framework of the World Trade Organisation to address this problem led to the conclusion of the Agreement on Trade-Related Aspects of Intellectual Property (the TRIPS Agreement). It contains, *inter alia*, provisions on the protection of trade secrets against their unlawful acquisition, use or disclosure by third parties, which are common international standards. All Member States, as well as the Union itself, are bound by this Agreement which was approved by Council Decision 94/800/EC.[5]

(5) Notwithstanding the TRIPS Agreement, there are important differences in the Member States legislation as regards the protection of trade secrets against their unlawful acquisition, use or disclosure by other persons. Thus, for example, not all Member States have adopted national definitions of trade secrets and/or unlawful acquisition, use or disclosure of a trade secret, so that the scope of protection is not readily accessible and differs throughout Member States. Furthermore, there is no consistency as regards the civil law remedies available in case of unlawful acquisition, use or disclosure of trade secrets as cease and desist orders are not always available in all Member States against third parties who are not competitors of the legitimate trade secret holder. Divergences also exist across the Member States with respect to the treatment of third parties who acquired the trade secret in good faith but subsequently come to learn, at the time of use, that their acquisition derived from a previous unlawful acquisition by another party.

(6) National rules also differ as to whether legitimate trade secret holders may seek the destruction of goods manufactured by third parties who use trade secrets unlawfully or the return or destruction of any documents, files or materials containing or implementing the unlawfully acquired or used trade secret. Also, applicable national rules on the calculation of damages do not always take account of the intangible nature of trade secrets, which makes it difficult to demonstrate the actual profits lost or the unjust enrichment of the

5 Council Decision of 22 December 1994 concerning the conclusion on behalf of the European Community, as regards matters within its competence, of the agreements reached in the Uruguay Round multilateral negotiations (1986–1994) (OJ L336, 23.12.1994, p. 1).

infringer where no market value can be established for the information in question. Only a few Member States allow for the application of abstract rules on the calculation of damages based on the reasonable royalty or fee which could have been due had a licence for the use of the trade secret existed. Additionally, many Member States rules do not guarantee the preservation of the confidentiality of a trade secret if the trade secret holder introduces a claim for alleged unlawful acquisition, use or disclosure of the trade secret by a third party, thus reducing the attractiveness of the existing measures and remedies and weakening the protection offered.

(7) The differences in the legal protection of trade secrets provided for by the Member States imply that trade secrets do not enjoy an equivalent level of protection throughout the Union, thus leading to fragmentation of the internal market in this area and weakening the overall deterrent effect of the rules. The internal market is affected in so far as such differences lower businesses' incentives to undertake innovation-related cross-border economic activity, including research or manufacturing cooperation with partners, outsourcing or investment in other Member States, which would depend on the use of the information protected as trade secrets. Cross-border network research and development as well as innovation-related activities, including related manufacturing and subsequent cross-border trade, are rendered less attractive and more difficult within the Union, thus also resulting in innovation-related inefficiencies at Union scale. In addition, higher business risk appears in Member States with comparatively lower levels of protection, where trade secrets may be stolen or otherwise unlawfully acquired more easily. This leads to inefficient allocation of capital to growth-enhancing innovation within the internal market because of the higher expenditure on protective measures to compensate for the insufficient legal protection in some Member States. It also favours the activity of unfair competitors who following the unlawful acquisition of trade secrets could spread resulting goods across the internal market. Legislative regime differences also facilitate the importation of goods from third countries into the Union through entry points with weaker protection, when the design, manufacturing or marketing of those goods rely on stolen or otherwise unlawfully acquired trade secrets. On the whole, such differences create a prejudice to the proper functioning of the internal market.

(8) It is appropriate to provide for rules at Union level to approximate the national legislative systems so as to ensure a sufficient and consistent level of ***civil*** redress across the internal market in case of unlawful acquisition, use or disclosure of a trade secret, ***without prejudice to the possibility for Member States to provide for more far reaching protection against the unlawful acquisition, use or disclosure of trade secrets as long as the safeguards protecting the interests of***

other parties are respected. For this purpose, it is important to establish a homogenous definition of a trade secret without restricting the subject matter to be protected against misappropriation. Such definition should therefore be constructed as to cover business information, technological information and know-how where there is both a legitimate interest in keeping confidential and a legitimate expectation in the preservation of such confidentiality. ***Such information or know-how should furthermore have commercial value, whether actual or potential. Such information or know-how has commercial value especially insofar as its unauthorized acquisition, use or disclosure is likely to harm the interest of the person lawfully controlling it in that it undermines his or her scientific and technical potential, business or financial interest, strategic positions or ability to compete***. By nature, such definition should exclude trivial information and should not extend to the knowledge and skills gained by employees in the normal course of their employment and which are ***generally*** known among or ***readily*** accessible to persons within the circles that normally deal with the kind of information in question.

(9) It is also important to identify the circumstances under which legal protection is justified. For this reason, it is necessary to establish the conduct and practices which are to be regarded as unlawful acquisition, use or disclosure of a trade secret. ~~Disclosure by Union institutions and bodies or national public authorities of business-related information they hold pursuant to the obligations of Regulation (EC) No. 1049/2001 of the European Parliament and of the Council[7] or to other rules on the access to documents should not be considered unlawful disclosure of a trade secret.~~

(10) In the interest of innovation and to foster competition, the provisions of this Directive should not create any exclusive right on the know-how or information protected as trade secrets. Thus, independent discovery of the same know-how and information remains possible ~~and competitiors of the trade secret holder are also free to reverse engineer any lawfully acquired product~~. ***Reverse engineering of a lawfully acquired product is a lawful means of acquiring information except when otherewise agreed by contract. The freedom of entering into such contractual arrangments may however be limited by law, such as it is the case of Article 5(3) of Directive 2009/24/EC of the European Parliament and of the Council.***[6]

~~7 Regulation (EC) No. 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L145, 31.5.2001, p. 43).~~

6 ***Directive 2009/24/EU of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, OJ L111, 5.5.2009, p. 16.***

(10a) Furthermore, the acquisition, use or disclosure of trade secrets, whenever imposed or permitted by law should not be treated as unlawful. As a result, the acquisition or disclosure of a trade secret by administrative or judicial authorities for the performance of their duties should be lawful. Also, disclosure by the Union's institution and bodies or national public authorities of business–related information they hold pursuant to the obligations of Regulation (EC) No. 1049/2001 of the European Parliament and of the Council[7] or to other rules on the public access to documents or on the transparency obligations of national public authorities should not be considered unlawful disclosure of a trade secret. The acquisition and disclosure of trade secrets in the context of the exercise of the rights of workers representatives to information, consultation and participation in accordance with Union and national law or practices, and the collective defence of the interests of workers and employers, including co-determination, is also excluded from the scope of unlawful acquisition, without prejudice of any duty of confidentiality imposed on the recipients of information so acquired. The acquisiton or disclosure of a trade secret in the context of statutory audits performed in accordance with Union or national law should not be considered an unlawful conduct either.

(10b) Media often make public data or information considered to be a trade secret by another party but the publication of which could be of public interest. As a result, it is important that measures and remedies provided for should not restrict the exercise of the freedom of expression and information (which encompasses media freedom and pluralism as reflected in Article 11 of the Charter of Fundamental Rights of the European Union) whenever legitimate.

(10c) This Directive should not affect the right of the social partners to enter into collective agreements, where foreseen under labour law, as regards duties not to disclose a trade secret or to limit its use and the consequences of a breach of such duties by the party subject to them, provided that any such collective agreement does not restrict the safeguards concerning the exceptions in this Directive when an application for measures, procedures and remedies provided for in this Directive for an alleged acquisition, use or disclosure of a trade secret shall be dismissed.

(11) In line with the principle of proportionality the measures and remedies intended to protect trade secrets should be tailored to meet the objective of a smooth functioning internal market for research and innovation without jeopardising other objectives and principles of public interest. In this respect, the measures and remedies ensure that competent judicial authorities account for ***factors such as*** the value of a trade secret, the seriousness of the conduct resulting

7 ***Regulation (EC) No. 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L145, 31.5.2001, p. 43).***

in the unlawful acquisition, use or disclosure of the trade secret as well as the impact of such conduct. It should also be ensured that the competent judicial authorities are provided with the discretion to weigh up the interests of the parties to the litigation, as well as the interests of third parties including, where appropriate, consumers.

(12) The smooth functioning of the internal market would be undermined if the measures and remedies provided for were used to pursue illegitimate intents incompatible with the objectives of this Directive. Therefore, it is important to ~~ensure that judicial authorities are empowered to sanction abusive behaviour by claimants who act~~ ***empower their judicial authorities to adopt appropriate measures with regard to abusive behaviour by claimants who act abusively or*** in bad faith and submit manifestly unfounded applications ***with, for instance, the purpose of unfairly delaying or restricting the respondent's access to the market or otherwise intimidating or harassing the respondent***. It is also important that measures and remedies provided for should not restrict ~~the freedom of expression and information (which encompasses media freedom and pluralism as reflected in Article 11 of the Charter of Fundamental rights of the European Union) or~~ whistleblowing activity. Therefore the protection of trade secrets should not extend to cases in which disclosure of a trade secret serves the public interest in so far as relevant misconduct or wrongdoing is revealed.

(13) In the interest of legal certainty and considering that legitimate trade secret holders are expected to exercise a duty of care as regards the preservation of the confidentiality of their valuable trade secrets and the monitoring of their use, it appears appropriate to restrict ***substantive claims or*** the possibility to initiate actions for the protection of trade secrets to a limited period ~~following the date on which the trade secret holders became aware, or had reason to become aware, of the unlawful acquisition, use or disclosure of their trade secret by a third party~~.

(14) The prospect of losing the confidentiality of a trade secret during litigation procedures often deters legitimate trade secret holders from instituting proceedings to defend their trade secrets, thus jeopardising the effectiveness of the measures and remedies provided for. For this reason, it is necessary to establish, subject to appropriate safeguards ensuring the right to a fair trial, specific requirements aimed at protecting the confidentiality of the litigated trade secret in the course of legal proceedings instituted for its defence. These should include the possibility to restrict ~~access to evidence or hearings, or to publish only the non-confidential elements of judicial decisions~~ ***the circle of persons entitled to have access to evidence or hearings, or to publish only the non-confidential elements of judicial decisions. In order to ensure that the right of the***

parties to a fair trial is not undermined, when the circle of persons entitled to have access to evidence or hearings is restricted, at least one person from each party and its respective lawyer or representative should form part of that circle. Also, in the case that the party is a legal person, the number of natural persons within that circle should be such as to ensure proper representation of that legal person. Such protection should remain in force after the legal proceedings have ended for as long as the information covered by the trade secret is not in the public domain.

(15) Unlawful acquisition of a trade secret by a third party could have devastating effects on its legitimate holder since once publicly disclosed it would be impossible for that holder to revert to the situation prior to the loss of the trade secret. As a result, it is essential to provide for fast**,** ***effective*** and accessible ~~interim~~ ***provisional*** measures for the immediate termination of the unlawful acquisition, use or disclosure of a trade secret, ***including when such trade secret is used for the provision of services***. Such relief must be available without having to await a decision on the substance of the case, with due respect for the rights of defence and the principle of proportionality having regard to the characteristics of the case in question. ***In certain instances, the alleged infringer may be permitted, subject to the lodging of guarantees, to continue to use the trade secret or disclose it, where there is little risk that it will enter the public domain***. Guarantees of a level sufficient to cover the costs and the injury caused to the respondent by an unjustified request may also be required, particularly where any delay would cause irreparable harm to the legitimate holder of a trade secret.

(16) For the same reason, it is also important to provide for measures to prevent further unlawful use or disclosure of a trade secret, ***including when such trade secret is used for the provision of services***. For prohibitory measures to be effective, their duration, when circumstances require a limitation in time, should be sufficient to eliminate any commercial advantage which the third party could have derived from the unlawful acquisition, use or disclosure of the trade secret. In any event, no measure of this type should be enforceable if the information originally covered by the trade secret is in the public domain for reasons that cannot be attributed to the respondent.

(17) A trade secret may be unlawfully used to design, manufacture or market goods, or components thereof, which may spread across the internal market, thus affecting the commercial interests of the trade secret holder and the functioning of the internal market. In those cases and when the trade secret in question has a significant impact on the quality, value or price of the resulting good or on reducing the cost, facilitating or speeding up its manufacturing or

marketing processes, it is important to empower judicial authorities to order ***effective and*** appropriate measures with a view to ensure that those goods are not put on the market or are removed from it. Considering the global nature of trade, it is also necessary that these measures include the prohibition of importing those goods into the Union or storing them for the purposes of offering or placing them on the market. Having regard to the principle of proportionality, corrective measures should not necessarily entail the destruction of the goods when other viable options are present, such as depriving the good of its infringing quality or the disposal of the goods outside the market, for example, by means of donations to charitable organisations.

(18) A person may have originally acquired a trade secret in good faith but only become aware at a later stage, including upon notice served by the original trade secret holder, that his or her knowledge of the trade secret in question derived from sources using or disclosing the relevant trade secret in an unlawful manner. In order to avoid that under those circumstances the corrective measures or injunctions provided for could cause disproportionate harm to that person, Member States should provide for the possibility, in appropriate cases, of pecuniary compensation being awarded to the injured party as an alternative measure, provided that such compensation does not exceed the amount of royalties or fees which would have been due had that person obtained authorisation to use the trade secret in question, for the period of time for which use of the trade secret could have been prevented by the original trade secret holder. Nevertheless, where the unlawful use of the trade secret would constitute an infringement of law other than that foreseen in this Directive or would be likely to harm consumers, such unlawful use should not be allowed.

(19) In order to avoid that a person who knowingly, or with reasonable grounds for knowing, unlawfully acquires, uses or discloses a trade secret benefit from such conduct and to ensure that the injured trade secret holder, to the extent possible, is placed in the position in which he or she would have been had that conduct not taken place, it is necessary to provide for adequate compensation of the prejudice suffered as a result of the unlawful conduct. The amount of damages awarded to the injured holder of the trade secret should take account of all appropriate factors, such as loss of earnings incurred by the trade secret holder or unfair profits made by the infringer and, where appropriate, any moral prejudice caused to the trade secret holder. As an alternative, for example where, considering the intangible nature of trade secrets, it would be difficult to determine the amount of the actual prejudice suffered, the amount of the damages might be derived from elements such as the royalties or fees which would have been due had the infringer requested authorisation to use the trade secret in question. The aim is not to introduce an obligation to provide for

punitive damages, but to ensure compensation based on an objective criterion while taking account of the expenses incurred by the holder of the trade secret, such as the costs of identification and research. ***The Directive shall not affect national principles on liability for violation of official duty.***

(20) To act as a supplementary deterrent to future infringers and to contribute to the awareness of the public at large, it is useful to publicise decisions, including where appropriate through prominent advertising, in cases concerning the unlawful acquisition, use or disclosure of trade secrets, as long as such publication does not result in the disclosure of the trade secret nor disproportionally affect the privacy and reputation of natural persons.

(21) The effectiveness of the measures and remedies available to trade secret holders could be undermined in case of non-compliance with the relevant decisions adopted by the competent judicial authorities. For this reason, it is necessary to ensure that those authorities enjoy the appropriate powers of sanction.

(22) In order to facilitate the uniform application of the measures for the protection of trade secrets, it is appropriate to provide for systems of cooperation and the exchange of information as between Member States, on the one hand, and between the Member States and the Commission on the other, in particular by creating a network of correspondents designated by Member States. In addition, in order to review whether these measures fulfil their intended objective, the Commission, assisted, as appropriate, by the European Observatory on the Infringements of Intellectual Property Rights, should examine the application of this Directive and the effectiveness of the national measures taken.

(23) This Directive respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union, notably the right to respect private and family life, the right to the protection of personal data, the freedom of expression and information, the freedom to choose an occupation and right to engage in work, the freedom to conduct a business, the right to property, the right to good administration, access to file and preservation of secrecy of business, the right to an effective remedy and to a fair trial and right of defence.

(24) It is important that the rights to privacy and personal data protection of any person ***whose personal data may be protected as a trade secret by the trade secret holder or of any person*** involved in litigation concerning the unlawful acquisition, use or disclosure of trade secrets and whose personal data are

processed are respected. Directive 95/46/EC of the European Parliament and of the Council[8] governs the processing of personal data carried out in the Member States in the context of this Directive and under the supervision of the Member States competent authorities, in particular the public independent authorities designated by the Member States. ***Thus, this Directive should not affect the rights and obligations laid down in Directive 95/46/EC, in particular the rights of the data subject to access his or her personal data being processed and to obtain rectification, erasure or blocking of the data where it is incomplete or inaccurate and, where appropriate, the obligation to process sensitive data in accordance with Article 8(5) of Directive 95/46/EC.***

(25) Since the objective of this Directive, to achieve a smooth functioning internal market through the establishment of a sufficient and comparable level of redress across the internal market in case of unlawful acquisition, use or disclosure of a trade secret, cannot be sufficiently achieved by Member States and can therefore, by reason of its scale and effects, be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty of European Union. In accordance with the principle of proportionality, as set out in that same Article, this Directive does not go beyond what is necessary in order to achieve that objective.

(26) This Directive should not aim to establish harmonised rules for judicial cooperation, jurisdiction, the recognition and enforcement of judgments in civil and commercial matters, or deal with applicable law. Other Union instruments which govern such matters in general terms should, in principle, remain equally applicable to the field covered by this Directive.

(27) This Directive should not affect the application of competition law rules, in particular Articles 101 and 102 of the Treaty on the Functioning of the European Union. The measures provided for in this Directive should not be used to restrict competition unduly in a manner contrary to that Treaty.

(28) The measures adopted to protect trade secrets against their unlawful acquisition, disclosure and use should not affect the application of any other relevant law in other areas including intellectual property rights, privacy, access to documents and the law of contract. However, where the scope of application

8 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 L281, 23.11.1995, p. 31).

of Directive 2004/48/EC of the European Parliament and of the Council[9] and the scope of this Directive overlap, this Directive takes precedence as lex specialis.

(29) The European Data Protection Supervision was consulted in accordance with Article 28(2) of Regulation (EC) No. 45/2001[10] and delivered an opinion on 12 March 2014.[11]

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

SUBJECT MATTER AND SCOPE

Article 1
Subject matter

This Directive lays down rules on the protection against the unlawful acquisition, ***use and*** disclosure ~~and use~~ of trade secrets.

Member State may provide, in compliance with the provisions of the Treaty, for more far-reaching protection against the unlawful acquisition, use or disclosure of trade secrets than that required in this Directive, provided that compliance with Articles 4, 5, Article 6(1), Article 7, the second subparagraph of Article 8(1), Articles 8(3), 8(4), 9(2), Articles 10, 12 and Article 14(3) is ensured.

Article 2
Definitions

For the purposes of this Directive, the following definitions shall apply:

(1) 'trade secret' means information which meets all of the following requirements:

(a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily

9 Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ L157, 30.4.2004, p. 45).

10 ***Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the community institutions and bodies and on the free movement of such data (OJ L8, 12.1.2001, p. 1).***

11 ***OJ C….***

accessible to persons within the circles that normally deal with the kind of information in question;
(b) has commercial value because it is secret;
(c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret;

(2) 'trade secret holder' means any natural or legal person lawfully controlling a trade secret;

(3) 'infringer' means any natural or legal person who has unlawfully acquired, used or disclosed trade secrets;

(4) 'infringing goods' means goods whose design, quality manufacturing process or marketing significantly benefits from trade secrets unlawfully acquired, used or disclosed.

CHAPTER II

~~UNLAWFUL A~~ACQUISITION, USE AND DISCLOSURE OF TRADE SECRETS

Article 3
Unlawful acquisition, use and disclosure of trade secrets

1. Member States shall ensure that trade secret holders are entitled to apply for the measures, procedures and remedies provided for in this Directive in order to prevent, or obtain redress for, the unlawful acquisition, use or disclosure of a trade secret.

2. The acquisition of a trade secret without the consent of the trade secret holder shall be considered unlawful whenever carried out ~~intentionally or with gross negligence~~ by:

(a) unauthorised access to, ~~or~~ copy***ing or appropriation*** of any documents, objects, materials, substances or electronic files, lawfully under the control of the trade secret holder, containing the trade secret or from which the trade secret can be deduced;
(b) ~~theft;~~
(c) ~~bribery;~~
(d) ~~deception;~~
(e) ~~breach or inducement to breach a confidentiality agreement or any other duty to maintain secrecy;~~

(f) any other conduct which, under the circumstances, is considered contrary to honest commercial practices.

3. The use or disclosure of a trade secret shall be considered unlawful whenever carried out, without the consent of the trade secret holder~~, intentionally or with gross negligence,~~ by a person who is found to meet any of the following conditions:

(a) has***ve*** acquired the trade secret unlawfully;
(b) ~~is~~ ***be*** in breach of a confidentiality agreement or any other duty ~~to maintain secrecy of~~ ***not to disclose*** the trade secret;
(c) ~~is~~ ***be*** in breach of a contractual or any other duty to limit the use of the trade secret.

4. The ***acquisition,*** use or disclosure of a trade secret shall also be considered unlawful whenever a person, at the time of ***acquisition,*** use or disclosure, knew or should, under the circumstances, have known that the trade secret was obtained ***directly or indirectly*** from another person who was using or disclosing the trade secret unlawfully within the meaning of the paragraph 3.

5. The ~~conscious and deliberate~~ production, offering or placing on the market of infringing goods, or import, export or storage of infringing goods for those purposes, shall ***also*** be considered an unlawful use of a trade secret ***when the person carrying out such activities knew, or should, under the circumstances, have known that the trade secret was used unlawfully within the meaning of paragraph 3.***

Article 4
Lawful acquisition, use and disclosure of trade secrets ***and exceptions***

1. The acquisition of trade secrets shall be considered lawful when obtained by any of the following means:

(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 ***who is free from any legally valid duty to limit the acquisition of the trade secrets***;
(c) ~~exercise of the rights of workers representatives to information and consultation in accordance with Union and national law and/or practices~~ ***any other practice which, under the circumstances, is in conformity with honest commercial practices***.

1a. The acquisition, use and disclosure of trade secrets shall be considered lawful to the extent that such acquisition, use or disclosure is required or allowed by Union or national law.

2. Member States shall ensure that there shall be no entitlement to the application for the measures, procedures and remedies provided for in this Directive are dismissed when the alleged acquisition, use or disclosure of the trade secret was carried out in any of the following cases:

(a) for making legitimate use of the right to freedom of expression and information;
(b) for the purpose of revealing ~~an applicant's~~ a misconduct, wrongdoing or illegal activity, provided that the alleged acquisition, use or disclosure of the trade secret was necessary for such revelation and that the respondent acted in the public interest;
(c) the trade secret was disclosed by workers to their representatives as part of the legitimate exercise of their representative functions, ***provided that such disclosure was necessary for that exercise***;
~~(d) for the purpose of fulfilling a non-contractual obligation;~~
(e) for the purpose of protecting a legitimate interest ***recognised by Union or national law***.

CHAPTER III

MEASURES, PROCEDURES AND REMEDIES

SECTION 1
GENERAL PROVISIONS

Article 5
General obligation

1. Member States shall provide for the measures, procedures and remedies necessary to ensure the availability of civil redress against unlawful acquisition, use and disclosure of trade secrets.

2. Those measures, procedures and remedies ***referred to in paragraph 1*** shall:

(a) be fair and equitable;
(b) not be unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays;
(c) be effective and dissuasive.

Article 6
Proportionality and abuse of litigation

1. ~~Member States shall ensure that the~~ ***The*** measures, procedures and remedies provided for in accordance with this Directive ~~are to~~ ***shall*** be applied ~~by the competent judicial authorities~~ in a manner that:

(a) is proportionate;
(b) avoids the creation of barriers to legitimate trade in the internal market; and
(c) provides for safeguards against their abuse.

2. Member States shall ensure that ~~where~~ competent judicial authorities ~~determine that~~ ***may, upon request of the respondent, apply appropriate measures as provided for in national law, where*** a claim concerning the unlawful acquisition, ***use or*** disclosure ~~or use~~ of a trade secret is manifestly unfounded and the applicant is found to have initiated the legal proceedings ***abusively or*** in bad faith ~~with the purpose of unfairly delaying or restricting the respondent's access to the market or otherwise intimidating or harrassing the respondent, such competent judicial authorities shall be entitled to take the following measures: (a) impose sanctions on the applicant, or (b) order~~. ***These measures may, as***

appropriate, include awarding damages to the respondent, imposing sanctions on the applicant or ordering the dissemination of the information concerning the decision taken in accordance with Article 14.

Member States may provide that these measures are dealt with in separate proceedings.

~~The measures referred to in the first subparagraph shall be without prejudice to the possibility for the respondent to claim damages, if Union or national law allows.~~

Article 7
Limitation period

Member States shall ~~ensure that~~ ***lay down the rules applicable to limitation periods for substantive claims or bringing*** actions for the application of the measures, procedures and remedies provided for in this Directive ~~may be brought within at least one year but not more than two years after the date on which the applicant became aware, or had reason to become aware, of the last fact giving rise to the action~~. ***Those rules shall determine when the limitation period begins to run, the duration of the limitation period and the circumstances under which the limitation period is interrupted or suspended. The duration of the limitation period shall not exceed six years.***

Article 8
Preservation of confidentiality of trade secrets in the course of legal proceedings

1. Member States shall ensure that the parties, their ~~legal~~ representatives, court officials, witnesses, experts and any other person participating in the legal proceedings relating to the unlawful acquisition, use or disclosure of a trade secret, or who has access to documents which form part of those legal proceedings, shall not be permitted to use or disclose any trade secret or alleged trade secret of which ***the competent judicial authorities have, in response to a duly reasoned application by the interested party, identified as confidential and of which*** they have become aware as a result of such participation or access.

The obligation referred to in the first subparagraph shall ***remain in force after the legal proceedings have ended. However, such obligation shall*** cease to exist in any of the following circumstances:

(a) where ~~in the course of the proceedings,~~ the alleged trade secret is found not to fulfil the requirements set ***out*** in point (1) of Article 2 ***by a final decision***;
(b) where over time, the information in question becomes generally known among or readily accessible to persons within the circles that normally deal with that kind of information.

2. Member States shall also ensure that the competent judicial authorities may, on a duly reasoned application by a party, take specific measures necessary to preserve the confidentiality of any trade secret or alleged trade secret used or referred to in the course of the legal proceedings relating to the unlawful acquisition, use or disclosure of a trade secret. ***Member states may also allow competent judicial authorities to take such measures on their own initiative.***

The measures referred to in the first subparagraph shall at least include the possibility:

(a) to restrict access to any document containing trade secrets ***or alleged trade secrets*** submitted by the parties or third parties, in whole or in part***, to a limited number of persons, provided that at least one person from each party, its respective lawyer or representative to the proceedings and court officials are given full access to such document***;
(b) to restrict access to hearings, when trade secrets ***or alleged trade secrets*** may be disclosed, and their corresponding records or transcript***, to a limited number of persons, provided that at least one person from each party, its respective lawyer or representative to the proceedings and court officials are given full access to such hearing, records or transcript***. ~~In exceptional circumstances, and subject to appropriate justification, the competent judicial authorities may restrict the parties' access to those hearings and order them to be carried out only in the presence of the legal representatives of the parties and authorised experts subject to the confidentiality obligation referred to in paragraph 1~~;
(c) to make available ***to third parties*** a non-confidential version of any judicial decision, in which the passages containing trade secrets have been removed.

Where, because of the need to protect a trade secret or an alleged trade secret and pursuant to point (a) of the second subparagraph of this paragraph, the competent judicial authority decides that evidence lawfully in the control of a party shall not be disclosed to the other party and where such evidence is material for the outcome of the litigation, the judicial authority may nevertheless authorise the disclosure of that information to the legal representatives of

the other party and, where appropriate, to authorised experts subject to the confidentiality obligation referred to in paragraph 1.

3. When deciding on the granting or the rejection of the application referred to in paragraph 2 and assessing its proportionality, the competent judicial authorities shall take into account ***the need to ensure the rights to an effective remedy and a fair trial,*** the legitimate interests of the parties and, where appropriate, of third parties, and any potential harm for either of the parties, and where appropriate third parties, resulting from the granting or rejection of such application.

4. Any processing of personal data pursuant to paragraphs 1, 2 and 3 shall be carried out in accordance with Directive 95/46/EC.

SECTION 2

~~INTERIM~~ PROVISIONAL AND PRECAUTIONARY MEASURES

Article 9
*~~Interim~~ **Provisional** and precautionary measures*

1. Member States shall ensure that the competent judicial authorities may, at the request of the trade secret holder, order any of the following ~~interim~~ ***provisional*** and precautionary measures against the alleged infringer:

(a) the cessation of or, as the case may be, the prohibition of the use or disclosure of the trade secret on ~~an interim~~ ***a provisional*** basis;
(b) the prohibition to produce, offer, place on the market or use infringing goods, or import, export or store infringing goods for those purposes;
(c) the seizure or delivery ***up*** of the suspected infringing goods, including imported goods, so as to prevent their entry into or circulation within the market.

2. Member States shall ensure that the judicial authorities may, ***as an alternative to the measures referred to in paragraph 1,*** make the continuation of the alleged unlawful ~~acquisition,~~ use or disclosure of a trade secret subject to the lodging of guarantees intended to ensure the compensation of the trade secret holder.

Article 10
Conditions of application and safeguards

1. Member States shall ensure that the competent judicial authorities have, in respect of the measures referred to in Article 9, the authority to require the applicant to provide evidence that may reasonably be considered available in order to satisfy themselves ***with sufficient degree of certainty*** that a trade secret exists, that the applicant is the ~~legitimate~~ trade secret holder and that the trade secret has been acquired unlawfully, that the trade secret is being unlawfully used or disclosed, or that an unlawful acquisition, use or disclosure of the trade secret is imminent.

2. Member States shall ensure that in deciding on the granting or rejecting of the application and assessing its proportionality, the competent judicial authorities shall be required to take into account the ***specific circumstances of the case. This assessment shall include, where appropriate, the*** value of the trade secret, the measures taken to protect the trade secret ***or other specific features of the trade secret, as well as*** the conduct of the respondent in acquiring, ***using or*** disclosing ~~or using~~ of the trade secret, the impact of the unlawful ***use or*** disclosure ~~or use~~ of the trade secret, the legitimate interests of the parties and the impact which the granting or rejection of the measures could have on the parties, the legitimate interests of third parties, the public interest and the safeguard of fundamental rights~~, including freedom of expression and information~~.

3. Member States shall ensure that the ~~interim~~ ***provisional*** measures referred to in Article 9 are revoked or otherwise cease to have effect, upon request of the respondent, if:

(a) the applicant does not institute proceedings leading to a decision on the merits of the case before the competent judicial authority, within a reasonable period determined by the judicial authority ordering the measures where the law of a Member State so permits or, in the absence of such determination, within a period not exceeding 20 working days or 31 calendar days, whichever is the longer;
(b) in the meantime, the information in question no longer fulfils the requirements of point (1) of Article 2, for reasons that cannot be attributed to the respondent.

4. Member States shall ensure that the competent judicial authorities may make the ~~interim~~ provisional measures referred to in Article 9 subject to the lodging by the applicant of adequate security or an equivalent assurance

intended to ensure compensation for any prejudice suffered by the respondent and, where appropriate, by any other person affected by the measures.

5. Where the ~~interim~~ ***provisional*** measures are revoked on the basis of point (a) of paragraph 3, where they lapse due to any act or omission by the applicant, or where it is subsequently found that there has been no unlawful acquisition, ***use or*** disclosure ~~or use~~ of the trade secret or threat of such conduct, the competent judicial authorities shall have the authority to order the applicant, upon request of the respondent or of an injured third party, to provide the respondent, or the injured third party, appropriate compensation for any injury caused by those measures.

Member States may provide that these measures are dealt with in separate proceedings.

SECTION 3

MEASURES RESULTING FROM A DECISION OF THE MERITS OF THE CASE

Article 11
Injunctions and corrective measures

1. Member States shall ensure that, where a judicial decision is taken finding an unlawful acquisition, use or disclosure of a trade secret, the competent judicial authorities may, at the request of the applicant order against the infringer:

(a) the cessation of or, as the case may be, the prohibition of the use or disclosure of the trade secret;
(b) the prohibition to produce, offer, place on the market or use infringing goods, or import, export or store infringing goods for those purposes;
(c) the adoption of the appropriate corrective measures with regard to the infringing goods.

2. The corrective measures referred to in point (c) of paragraph 1 shall include:

(a) a declaration of infringement;
(b) recall of the infringing goods from the market;
(c) depriving the infringing goods of their infringing quality;
(d) destruction of the infringing goods or, where appropriate, their withdrawal from the market, provided that such action ***measure*** does not undermine the protection of the trade secret in question;

(e) the destruction of all or part of any document, object, material, substance or electronic file containing or implementing the trade secret or, where appropriate, the delivery up to the trade secret holder ***applicant*** of all or part of those documents, objects, materials, substances and electronic files.

3. Member States ~~shall ensure~~ ***may provide*** that, when ordering the withdrawal of the infringing goods from the market, the judicial authorities may order, at the request of the trade secret holder, that the goods be delivered up to holder or to charitable organisations ~~under conditions to be determined by the judicial authorities aimed at ensuring that the goods in question do not re-enter the market~~.

4. The judicial authorities shall order that ~~those~~ ***the*** measures ***referred to in point (c) of paragraph 1*** be carried out at the expense of the infringer, unless there are particular reasons for not doing so. These measures shall be without prejudice to any damages that may be due to the trade secret holder by reason of the unlawful acquisition, use or disclosure of the trade secret.

Article 12
Conditions of application, safeguards and alternative measures

1. Member States shall ensure that, in considering a request for the adoption of the injunctions and corrective measures provided for in Article 11 and assessing their proportionality, the competent judicial authorities ***shall be required to*** take into account ***the specific circumstances of the case. This assessment shall include, where appropriate,*** the value of the trade secret, the measures taken to protect the trade secret***, or other specific features of the trade secret, as well as*** the conduct of the infringer in acquiring, ***using or*** disclosing ~~or using~~ the trade secret, the impact of the unlawful ***use or*** disclosure ~~or use~~ of the trade secret, the legitimate interests of the parties and the impact which the granting or rejection of the measures could have on the parties, the legitimate interests of third parties, the public interest and the safeguard of fundamental rights~~, including freedom of expression and information~~.

When the competent ***judicial*** authorities limit the duration of the measure referred to in point (a) ***and (b)*** of Article 11(1), such duration shall be sufficient to eliminate any commercial or economic advantage that the infringer could have derived from the unlawful acquisition, ***use or*** disclosure ~~or use~~ of the trade secret.

2. Member States shall ensure that the measures referred to in point (a) ***and (b)*** of Article 11(1) are revoked or otherwise cease to have effect, upon request of

the respondent if in the meantime the information in question no longer fulfils the conditions of point (1) of Article 2 for reasons that cannot be attributed to the respondent.

3. Member States shall provide that, at the request of the person liable to be subject to the measures provided for in Article 11, the competent judicial authority may order pecuniary compensation to be paid to the injured party instead of applying those measures if all the following conditions are met:

(a) the person concerned ~~originally acquired knowledge of~~ ***at the time of use or disclosure neither knew nor had reason, under the circumstances, to know that*** the trade secret ~~in good faith and fulfils the conditions of Article 3(4)~~ ***was obtained from another person who was using or disclosing the trade secret unlawfully***;
(b) execution of the measures in question would cause that person disproportionate harm;
(c) pecuniary compensation to the injured party appears reasonably satisfactory.

When the pecuniary compensation is ordered instead of the order referred to in point (a) ***and (b)*** of Article 11(1), such pecuniary compensation shall not exceed the amount of royalties or fees which would have been due, had that person requested authorisation to use the trade secret in question, for the period of time for which use of the trade secret could have been prohibited.

Article 13
Damages

1. Member States shall ensure that the competent judicial authorities, on the application of the injured party, order the infringer who knew or ought to have known that he or she was engaging in unlawful acquisition, ***use or*** disclosure ~~or use~~ of a trade secret, to pay the trade secret holder damages ~~commensurate to~~ ***for*** the actual prejudice suffered ***as a result of the infringement***.

In accordance with their national law and practice, Member States may restrict the liability for damages of employees towards their employers for the unlawful acquisition, use or disclosure of a trade secret of the employer when they act without intent.

2. When setting the damages ***pursuant to paragraph 1***, the competent judicial authorities shall take into account all appropriate factors, such as the negative economic consequences, including lost profits, which the injured party has

suffered, any unfair profits made by the infringer and, in appropriate cases, elements other than economic factors, such as the moral prejudice caused to the trade secret holder by the unlawful acquisition, use or disclosure of the trade secret.

3. However, the competent judicial authorities may also, in appropriate cases, set the damages as a lump sum on the basis of elements such as, at a minimum, the amount of royalties or fees which would have been due if the infringer had requested authorisation to use the trade secret in question.

Article 14
Publication of judicial decisions

1. Member States shall ensure that, in legal proceedings instituted for the unlawful acquisition, use or disclosure of a trade secret, the competent judicial authorities may order, at the request of the applicant and at the expense of the infringer, appropriate measures for the dissemination of the information concerning the decision, including publishing it in full or in part.

2. Any measure referred to in paragraph 1 of this Article shall preserve the confidentiality of trade secrets as provided for in Article 8.

3. In deciding whether to order a ~~publicity~~ measure ***referred to in paragraph 1*** and assessing its proportionality, the competent judicial authorities shall take into account ***whether the information on the infringer would allow to identify a natural person and, if so, whether publication of that information would be justified, in particular in light of the following criteria***: the possible harm that such measure may cause to the privacy and reputation of the infringer, ~~whenever the infringer is a natural person, as well as the value of the trade secret,~~ the conduct of the infringer in acquiring, disclosing or using the trade secret~~, the impact of the unlawful disclosure or use of the trader secret~~ and the likelihood of further unlawful use or disclosure of the trade secret by the infringer. ***The competent judicial authorities shall also take into account, where appropriate, other circumstances, in particular the value of the trade secret and the impact of the unlawful acquisition, disclosure or use of the trade secret.***

CHAPTER IV

SANCTIONS, REPORTING AND FINAL PROVISIONS

Article 15
Sanctions for non-compliance with the obligations set out in this Directive

Member States shall ensure that the competent judicial authorities may impose sanctions on ~~the parties, their legal represenatives and~~ any ~~other~~ person who fails or refuses to comply with any measure adopted pursuant to Articles 8, 9, and 11.

The sanctions provided for shall include the possibility to impose recurring penalty payments in case of non-compliance with a measure adopted pursuant to Articles 9 and 11.

The sanctions provided for shall be effective, proportionate and dissuasive.

Article 16

Exchange of information and correspondents

For the purpose of promoting cooperation, including the exchange of information, among Member States and between Member States and the Commission, each Member State shall designate one or more national correspondents for any question relating to the implementation of the measures provided for by this Directive. It shall communicate the details of the national correspondent(s) to the other Member States and the Commission.

Article 17
Reports

1. By XX XX 20XX [*three years after the end of the transposition period*], the ~~European Union Trade Marks and Designs Agency~~ ***Office for Harmonisation in the Internal Markets (Trade Marks and Designs)***, in the context of the activities of the European Observatory on Infringements of Intellectual Property Rights, shall prepare an initial report on the litigation trends regarding the unlawful acquisition, use or disclosure of trade secrets pursuant to the application of this Directive.

2. By XX XX 20XX [*four years after the end of the transposition period*], the Commission shall draw up an intermediate report on the application of this

Directive and submit it to the European Parliament and the Council. This report shall take due account of the report ~~prepared by the European Observatory on Infringements of Intellectual Property Rights~~ ***referred to in paragraph 1***.

3. By XX XX 20XX [*eight years after the end of the transposition period*], the Commission shall carry out an evaluation of the effects of this Directive and submit a report to the European Parliament and the Council.

Article 18
Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by XX XX 20XX [*24 months after the date of adoption of this Directive*] at the latest. They shall forthwith communicate to the Commission the text of those provisions.

When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

Article 19
Entry into force

This Directive shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

Article 20
Addressees

This Directive is addressed to the Member States.

INDEX