OECD publishing

Please cite this paper as:

Schultz, M. and D. Lippoldt (2014-01-30), "Approaches to Protection of Undisclosed Information (Trade Secrets): Background Paper", *OECD Trade Policy Papers*, No. 162, OECD Publishing, Paris.
http://dx.doi.org/10.1787/5jz9z43w0jnw-en

OECD Trade Policy Papers No. 162

Approaches to Protection of Undisclosed Information (Trade Secrets)

BACKGROUND PAPER

Mark F. Schultz,

Douglas C. Lippoldt

OECD

OECD TRADE POLICY PAPERS

The OECD Trade Policy Paper series is designed to make available to a wide readership selected studies by OECD staff or by outside consultants. This series continues that originally entitled OECD Trade Policy Working Papers.

This document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

This document has been declassified on the responsibility of the Working Party of the Trade Committee under the OECD reference number TAD/TC/WP(2013)21/FINAL.

Comments on the series are welcome and should be sent to tad.contact@oecd.org.

OECD TRADE POLICY PAPERS
are published on www.oecd.org/trade

© OECD (2014)

You can copy, download or print OECD content for your own use, and you can include excerpts from OECD publications, databases and multimedia products in your own documents, presentations, blogs, websites and teaching materials, provided that suitable acknowledgment of OECD as source and copyright owner is given. All requests for commercial use and translation rights should be submitted to *rights@oecd.org*.

Abstract

Approaches to Protection of Undisclosed Information (Trade Secrets) – Background Paper

This paper takes stock of the available legal protection for trade secrets (undisclosed information) in a broad sample of countries. Drawing on national and international material, the paper develops and presents an indicator of the stringency of protection of trade secrets (the Trade Secrets Protection Index) and provides an assessment of variation in the available protection. The result is a finding that while the sample countries have some similarities, notably with respect to definition and scope of trade secrets, they have many more substantial dissimilarities with respect to implementation of protection for trade secrets. For example, differences are particularly pronounced in evidence gathering and discovery, protection of trade secrets during litigation, technology transfer requirements and the effectiveness of legal systems with respect to enforcement. This diversity is reflected in the wide range of scores in the Trade Secrets Protection Index. Such variation in the stringency of protection for trade secrets may influence firm-level decision-making and may have implications for some aspects of economic performance (in particular, in relation to innovation).

Keywords: Trade Secrets, Intellectual Property Rights, Trade Secrets Protection Index.

JEL classification: O34, F13.

Acknowledgements

This paper benefitted from the data, insights and references shared by a number of colleagues. Thanks are due in particular to Jean Bergevin, Eric Claeys, Beate Devoghele-Lalk, Allen Dixon, Carsten Fink, Mariano Fernandez-Salas, Manuel Godinho de Matos, Brian Kahin, Clarisse Legendre, Alan C. Marco, Wolf Meier-Ewert, Douglas Nelson, Jorge Novais Gonçalves, Walter Park, James Pooley, Thomas Respess, Raed Safadi, Sharon Sandeen, Aaron Smethurst, Piotr Stryszowski, Kitisri Sukhapinda, Anthony Taubman, Andy Toole, Raymundo Valdes, Pedro Velasco-Martins and Trudy Witbreuk, as well as other colleagues at the European Commission, Office of the US Trade Representative, US Patent and Trademark Office, Working Party of the OECD Trade Committee, World Intellectual Property Organization and World Trade Organization, and participants at the Trade Secrets Works-in-Progress Workshop at Elon University in November 2012. Jacqueline Maher capably formatted the paper for publication. Daniel Evans, Dennis Leach and Tania Linares provided excellent research assistance. The authors remain responsible for any errors or omissions.

Table of contents

Acknowledgements 2
Executive Summary 5
1. Introduction 6
2. The International Framework and the Definition of Trade Secrets 6
3. Literature Review 9
3.1 The Conceptual Debate Regarding Trade Secret Law 10
3.2 Economics and Trade Secret Law 11
4. Method 14
5. Survey of Legal Provisions and Practices 16
5.1 Similarities Among Countries 16
5.2 Key Points of Divergence 17
5.3 A Deeper Look at Countries in the Survey 20
6. Trade Secret Protection Index 21
6.1 Index Composition 23
6.2 TSPI - Index Results 23
7. Conclusions 24
References 35
Annex 1: Country Charts and Preliminary Index Scoring 49
Overview 49
Annex Chart 50
Australia 50
Brazil 57
Colombia 82
France 89
Germany 96
India 103
Israel 110
Italy 116
Japan 124
Korea 131
Malaysia 138
New Zealand 145
Peru 152
Russian Federation 159
Singapore 166
South Africa 173
Sweden 180
United Kingdom 187
United States 193
Annex Table 200

Annex 2: Detailed Overviews for the BRICS and a Sample of OECD Countries 207
Introduction 207
BRICS and OECD Country Overviews 208
Australia 208
Brazil 215
China 224
France 237
Germany 244
India 251
Israel 256
Italy 262
Japan 267
Korea 275
New Zealand 281
Russian Federation 288
South Africa 298
Sweden 303
United Kingdom 310
United States 317

Executive Summary

This background paper takes stock of the available legal protection for trade secrets (undisclosed information) and presents a method for the assessment of the stringency of available protection. The objective is to better understand the nature of the protection and how it might vary across a diverse sample of countries. This information will provide an essential input for the second phase of the project that will consider the relationship of the stringency of trade secrets protection to relevant aspects of economic performance.

The paper prepares the foundation for the work by defining trade secrets and presenting the international framework. Trade secrets are defined, essentially, as concerning information that is secret, that has commercial value because of its status as secret, and that is the subject of reasonable efforts to protect the secrecy. This definition is in line with the approach presented in the World Trade Organization's Agreement on Trade-Related Aspects of Intellectual Property Rights, the first multilateral agreement to require protection for trade secrets. The paper then moves to consider the current economic and legal literature, which is fairly substantial in terms of legal scholarship but less complete with respect to economic analysis.

Using a structured comparative approach, the paper examines national legal regimes for a diverse sample of countries (including the BRICS, five other partner countries and 11 OECD countries). Drawing on national and international material, the paper develops and presents an indicator of the stringency of protection of trade secrets (the Trade Secrets Protection Index). The paper provides a taxonomy of elements of protection for trade secrets, text tables describing the main characteristics of the regimes in the sample countries, and detailed narrative overviews for the trade secrets legal regimes in the BRICS and OECD countries in the sample. These items constitute substantial contributions towards the deliverables under the OECD trade secrets project.

The result of this assessment is a finding that while the sample countries have some similarities, notably with respect to definition and scope of trade secrets, they have many more substantial dissimilarities with respect to implementation of protection for trade secrets. For example, differences are particularly pronounced in evidence gathering and discovery, protection of trade secrets during litigation, technology transfer requirements and the effectiveness of legal systems with respect to enforcement, among other differences. This diversity is reflected in the wide range of scores in the preliminary Trade Secrets Protection Index. Such variation in the stringency of protection for trade secrets may influence firm-level decision-making and may have implications for some aspects of economic performance (in particular, in relation to innovation).

The next phase of the OECD trade secrets project will focus on economic analysis. It will be based on dual approaches: a qualitative assessment and a quantitative assessment. The objective will be to examine empirically the relationship between the stringency of protection for trade secrets and performance concerning the types of economic indicators that may be hypothesised to be responsive to variation in protection of trade secrets. Such an assessment may help policy-makers in the identification of policy options for improved economic performance with respect to trade secrets.

1. Introduction

This background paper takes stock of the available legal protection for trade secrets and presents a method for the assessment of the stringency of available protection. The objective is to better understand the nature of the protection and how it might vary across a diverse sample of countries. This information will provide an essential input for the second phase of the project that will consider the relationship of the stringency of trade secrets protection to relevant aspects of economic performance.

The present paper is structured around an introduction, five substantive sections, and a conclusion. In section 2, the paper prepares the foundation for the work by defining trade secrets and presenting the international framework. It then moves to consider the current legal and economic literature. The following section presents an overview of the method employed in the analysis. Using a comparative approach, the fifth section of the paper examines national legal regimes for a diverse sample of countries. Drawing on the national and international material, the paper proposes a set of elements for inclusion in an indicator of the stringency of protection of trade secrets. The subsequent section presents an implementation of this method for the sample countries. The conclusions provide some observations on the results and next steps in the project. There are two substantial annexes to the paper. Annex 1 provides a snapshot of the key elements of trade secret protection in each of the sample countries. Annex 2 provides a detailed overview of trade secrets protection in the BRICS and OECD countries covered by the sample.

The project has employed a sampling approach in order to gauge the variation in available trade secret protection. The sample of countries is structured to capture diversity in terms of: (1) approaches to protection of trade secrets (i.e. in terms of civil, criminal and common law), (2) geography (e.g. country location, size and endowments), (3) income level (upper middle and high income countries) and (4) country grouping (i.e. OECD or partner status). A further constraint was availability of data needed to conduct the research. The resulting sample covers the BRICS and five other partner countries plus a sample of 11 OECD countries, including: Australia, Brazil, Bulgaria, China, Colombia, France, Germany, India, Israel, Italy, Japan, Korea, Malaysia, New Zealand, Peru, Russian Federation, Singapore, South Africa, Sweden, United Kingdom and United States. The report focuses on the situation in these countries for the most recent period available, generally 2010.

2. The International Framework and the Definition of Trade Secrets

The countries in the sample are all members of the World Trade Organization (WTO) and are subject to the provisions of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). The TRIPS Agreement was the first international agreement to protect trade secrets expressly (Box 1). The approach laid out in the TRIPS Agreement is based on the notion that protection against unfair competition should include protection for undisclosed information. In presenting this approach, the TRIPS Agreement makes reference to the prior-existing protection against unfair competition as presented in the Paris Convention for the Protection of Industrial Property (Box 2), a convention that is administered by the World Intellectual Property Organization.

Although trade secrets are confidential, they are also commercial. For a trade secret to have any practical value, the owner usually must share it in order to collaborate with a limited group of employees and business partners. Laws thus expect and account for a certain amount of protected disclosure, within a constrained circle. Nevertheless, even if trade secrets are not "secret" in the strictest sense of the term, they must in fact remain non-public and known only

to a limited number of people. The definition of trade secrets thus is broadly similar among countries, addressing their dual nature as confidential but commercial.

Box 1. The TRIPS Agreement on Undisclosed Information

Protection of undisclosed information is addressed in Article 39 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) of the World Trade Organization (WTO). This agreement entered into force on 1 January 1995 and established an international standard requiring WTO Members to protect undisclosed information including agricultural and pharmaceutical test data.

Section 7: Protection of Undisclosed Information, Article 39

1. In the course of ensuring effective protection against unfair competition as provided in Article 10bis of the Paris Convention (1967), Members shall protect undisclosed information in accordance with paragraph 2 and data submitted to governments or governmental agencies in accordance with paragraph 3.[1]

2. Natural and legal persons shall have 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] so long as such information:

(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.

3. 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.

Source: Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), WTO.

The similarities among countries in defining trade secrets correspond well with the three requirements of Article 39 of TRIPS. In fact, on this matter, TRIPS reflected then-current practice in many countries and it has shaped subsequent law-making. In practice, the TRIPS requirements for trade secrets are now generally applied in law as follows:

- *Secrecy*. The information protected must actually be secret. Secrecy need not be absolute. The trade secret owner may share the information with employees and business partners. Secrecy requires instead that the information must not be readily publically accessible and

1 These paragraph references refer to paragraphs 2 and 3 of Article 39 of the TRIPS Agreement.

2 At this point in the original text, there is a footnote, numbered 10, that states:
For the purpose of this provision, "a manner contrary to honest commercial practices" shall mean at least practices such as breach of contract, breach of confidence and inducement to breach, and includes the acquisition of undisclosed information by third parties who knew, or were grossly negligent in failing to know, that such practices were involved in the acquisition.

that it is revealed to others only under conditions that maintain secrecy with respect to the broader public.[3]

- *Commercial Value.* The information must have economic value as a result of its being secret. Trade secret law most typically protects commercial information; that information must derive some utility from being kept secret.
- *Reasonable Efforts to Maintain Secrecy.* The information must be the subject of reasonable efforts on the part of the rights holder to maintain its secrecy. By its nature, a trade secret claim arises when measures to protect the secret have failed. Thus, the law does not require one who claims a trade secret to be entirely successful at protecting it. However, the law does require the owner to make some efforts to maintain secrecy. In national laws, the necessary effort is often broadly described as "reasonable," in keeping with Article 39 of TRIPS. However, some countries impose more specific, additional obligations, which might be characterized as a particular implementation of the broad reasonableness requirement. For example, some common law countries require that the defendant have a contractual or implied obligation to keep the information secret. Other countries require written agreements with recipients and confidentiality notices.

These three conditions define trade secrets in a manner covering a potentially very large scope of economic activity.[4] Still, the resulting definition has potentially important practical implications as pointed out by Maskus (2000), who notes that trade secrets "are not protected against learning by fair means, such as independent creation, reverse engineering or reading public documents." In other words, trade secrecy does not provide an exclusive right to use of the information, so long as a second party obtains the information fairly or it enters the public domain by fair means. Thus, unlike patented inventions or copyright protected content, trade secrets are not protected for a statutory time limit and they can run out in the regular course of competition. The range of subject matter covered by trade secrets may be open-ended, though often trade secrets fall into one of two broad categories: technical information (e.g. technical plans and formulae) and confidential business information (e.g. customer lists and marketing strategies) (Almeling et al., 2010).

The TRIPS Agreement requires that WTO members put in place national systems to protect trade secrets against acts of unfair competition (Sandeen, 2011). WTO members comply with this obligation in a variety of ways. The fact that TRIPS Article 39 does not set forth a detailed regime for protection is associated with substantial variation between countries in the means employed to provide the TRIPS -mandated protection. In some instances, countries have implemented express legislation. In others, the obligation is met by laws that include misappropriation via such means as breach of contract, inducement of others to breach contracts and acquisition by third parties of information known to be disclosed dishonestly (or where it was negligent not to know). This variation can affect the ways businesses and workers conduct their affairs and thus there are reasons to believe that the legal protection of trade secrets may have important economic effects.

3 Moreover, as Pooley (1997) notes, the idea need not be unique to its owner. Several competitors could have developed the same idea via independent innovation and sought to protect it as a trade secret. This possibility is one factor differentiating trade secrets from patents.

4 For descriptive convenience this paper will employ the term "trade secrets" as encompassing "undisclosed information."

Box 2. Paris Convention for the Protection of Industrial Property, Articles 1 and 10*bis*, 1967[5]

In protecting Trade Secrets, the TRIPS Agreement references the protection provided in the Paris Convention against unfair competition. Article 10bis of the Paris Convention highlights the nature of protection against unfair competition. Article 1 of the Paris Convention is included here to provide context concerning what is meant by "union" (see article 1.1). Article 1 also defines the scope of industrial property originally covered, which the TRIPS Agreement extends by explicitly providing for protection of undisclosed information.

Selected articles of the Paris Convention

Article 1: Establishment of the Union; Scope of Industrial Property

(1) The countries to which this Convention applies constitute a Union for the protection of industrial property.

(2) The protection of industrial property has as its object patents, utility models, industrial designs, trademarks, service marks, trade names, indications of source or appellations of origin, and the repression of unfair competition.

(3) Industrial property shall be understood in the broadest sense and shall apply not only to industry and commerce proper, but likewise to agricultural and extractive industries and to all manufactured or natural products, for example, wines, grain, tobacco leaf, fruit, cattle, minerals, mineral waters, beer, flowers, and flour.

(4) Patents shall include the various kinds of industrial patents recognized by the laws of the countries of the Union, such as patents of importation, patents of improvement, patents and certificates of addition, etc.

Article 10bis: Unfair Competition

(1) The countries of the Union are bound to assure to nationals of such countries effective protection against unfair competition.

(2) Any act of competition contrary to honest practices in industrial or commercial matters constitutes an act of unfair competition.

(3) The following in particular shall be prohibited:

(i) all acts of such a nature as to create confusion by any means whatever with the establishment, the goods, or the industrial or commercial activities, of a competitor;

(ii) false allegations in the course of trade of such a nature as to discredit the establishment, the goods, or the industrial or commercial activities, of a competitor;

(iii) indications or allegations the use of which in the course of trade is liable to mislead the public as to the nature, the manufacturing process, the characteristics, the suitability for their purpose, or the quantity, of the goods.

Source: World Intellectual Property Organization.

3. Literature Review

The legal and economic literature on trade secrets is relatively limited in quantity and scope compared to the literature regarding other forms of intellectual property. The portions most relevant to this paper fall into two categories: i) conceptual theories of trade secret law and ii) economic assessments regarding the effects of trade secret law.

5 The Paris Convention entered into force on 26 April 1970. These articles remained unchanged in the subsequent edition of the Paris Convention (1979).

3.1 The Conceptual Debate Regarding Trade Secret Law

There is a robust debate in the legal literature as to whether trade secret law is based on relational obligations (for example, contract, employment status, or fiduciary duty); property rights; fairness and equity; or unfair competition law tort or delict. A fifth position offered by Bone (1998) and characterized by Claeys (2011) as "trade secrecy nihilism" contends that trade secret law lacks any unified theory, but is rather a collection of approaches and norms regarding the protection of business information. Claeys (2011) and Risch (2007) survey this debate in the context of current US law, Richardson et al., (2012) examine the historical evolution and debate among various conceptions in the law of the England and other common law jurisdictions, while Knobel (2000) provides an example of the debate in the context of South African law, where trade secret protection is based on the ancient Roman Lex Aquilia. Views of the basis for trade secret protection vary both within and between countries. For example, Claeys (2011), in contrast to Bone (1998), contends that the proprietary account does the best job of explaining the structure of trade secret protection in the United States, including rights and remedies. By contrast, Gurry (2012) explains that under English law trade secrets are protected by an action for breach of confidence under a relationship-based view of trade secrecy.

The differing conceptions of trade secret law result from different normative and conceptual premises. The US Supreme Court observed, citing John Locke and Blackstone, that the "perception of trade secrets as property is consonant with a notion of 'property' that extends beyond land and tangible goods and includes the products of an individual's 'labor and invention.'"[6] The Court further observed that "[t]rade secrets have many of the characteristics of more tangible forms of property"[7]; in particular, the Court noted that they are alienable in various ways, which is a hallmark of property rights. Some scholars contend that trade secrets cannot be property because they do not provide exclusive rights against the world (Bone, 1998). However, Claeys describes trade secrets as simply a different form of property right, like water rights rather than rights in land (Claeys, 2013). In this conception, they are usufructory rights, which confer rights to use a resource and to be free from interference with use, but which do not confer the right to exclude those who derive benefits from the resource by their *independent* efforts. By contrast, some jurisdictions ground trade secret rights in duties between the parties. Thus, for example, UK trade secrecy law sanctions breaches of confidence where the information was imparted in confidence, thus giving rise to a duty (Gurry, 2012).

The answer to this debate regarding the conceptual basis for trade secret law can be consequential. For example, the US Supreme Court's conclusion that trade secrets are protected as property had the implication that the US Government's forcing of disclosure of such information may require compensation under the US Constitution. Whereas, most European countries do not conceive of trade secrets as property and, therefore, they are not subject to the EU Enforcement Directive, which is also significant. The Enforcement Directive provides for certain procedures and remedies that facilitate the investigation and pursuit of intellectual property claims, for example.

6 Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1002-1003 (1984).

7 Ibid.

3.2 Economics and Trade Secret Law

Incentives

The economic literature describes the economic justification for trade secret law in terms of the incentives it provides. It describes three types of incentives. First, it provides incentives to invent and to invest in the development of valuable business information. Second, it relieves businesses of the need to invest in some costly measures to prevent breach of security. Third, it encourages businesses to engage in wider (albeit limited) dissemination of information than they otherwise would, thus increasing the likelihood of knowledge spillovers. Given the importance of trade secrets in many economies (Box 3), the potential impacts of such incentives would appear to be significant.

A number of studies indicate that protection of trade secrets can encourage the development of inventions and valuable information by helping to secure the return on the investment in creating such innovations. Kitch (1980) characterizes the incentive in terms of risk reduction: trade secrets are particularly at risk from theft because they have a low rate of depreciation. Friedman et al. (1991) similarly view the incentive effect as increasing the return to research and development by lowering the cost of protection. Others see the incentive function as similar to patents, where trade secrets essentially serve as a substitute for patents where the latter are unavailable or too expensive. Maskus (2000) and Friedman et al. (1991) argue that that trade secrets can substitute for patents and provide incentives to innovate, where: 1) an invention is unpatentable, but hard to imitate, such that there is value in keeping the information confidential (e.g. a customer list), 2) a firm may prefer to avoid the public disclosure required by a patent, and 3) where a firm may wish to avoid the cost of obtaining a patent. Still others see the incentive-to-invest arising from competitive effects. Lemley (2011) observes that protection of trade secrets can help innovators to maintain a competitive advantage such as might be obtained via a unique process of production or product; this can contribute to profitability and thereby provides incentives for further investment in innovation.

Some scholars critique the incentive-to-invest account. Risch (2007 and 2011) points out that trade secrets can only protect information that firms already can, and do, keep secret. They thus create no new ability to keep information secret. He argues that firms already have an incentive to invest in creating secret information. In this view, trade secret protection has a relatively small marginal effect on investment in research and development. They serve to assure firms that they may be able to secure an injunction to "rescue" a secret that that is threatened, stolen, or disclosed, or to secure damages. Bone (1998) also critiques the incentive-to-invest theory as overestimating benefits and underestimating the cost of keeping secrets.

Other studies point to a second justification for trade secrets, noting that the provision of adequate legal protection reduces the need to invest in inefficient and costly protection for trade secrets beyond the requirements of the law. As Friedman et al. (1991) observe, the availability of trade secret protection discourages use of less efficient alternative approaches to protection (e.g. hiring only family members or paying wage premia to prevent employee movement) and also inefficient activity by competitors to discover trade secrets (e.g. bribery or espionage). As Risch (2007) points out, both trade secret owners and competitors are channelled into more efficient behaviour. The owner optimizes, rather than maximizes, security. The competitor spends less money in attempting to appropriate the secret.

A third justification for trade secrets found in the literature relates, somewhat ironically, to their effects in encouraging knowledge dissemination, at least as compared to absolute

secrecy. As Lemley (2011) argues, trade secret protection enlarges the circle of people to whom it is safe to reveal information. Thus employees who may eventually depart are more likely to have the opportunity to learn from the trade secret. Even if they do not misappropriate the original secret, they may benefit from their enhanced stock of knowledge, as may future employers. Risch (2007) also contends that the incentives to rely on legal rather than physical means to guard secrets encourage owners to employ lesser levels of protection, thus increasing the likelihood of "leakage," and subsequently knowledge dissemination. In a further study, Png (2012a) found that some US states enacting increased trade secret protection may have experienced relatively modest declines in the mobility of postgraduate engineers and scientists (e.g. due to enforcement of contractual requirements concerning non-competition); this in turn might slow the pace spillover effects. However, this effect might be mitigated depending on presumptions states make related to possible disclosures (e.g. depending on whether they apply a doctrine of "inevitable disclosure"). Moreover, the possible costs to innovation due to any reduction in spillovers from reduced mobility of these most-qualified personnel may be off-set to some extent by the benefits to innovation from increased incentives to invest in R&D.

Box 3. References to the Economic Importance of Trade Secrets

While the secrecy requirements make it difficult to estimate the economic value of trade secrets, some indications are available from the literature.[8] Some estimates for the United States in the past decade, for example, put the annual cost of trade secret theft to US firms as high as USD 300 billion (Almeling et al., 2010). In a further example, interviews with members of the European Chemical Industry Council revealed that misappropriation of a trade secret or confidential business information could often entail a loss of revenue for a firm of up to 30% and sometimes much more (CEFIC, 2012). Clearly, businesses suffer when trade secrets are compromised. They risk potential losses to reputation, image, goodwill, competitive advantage, core technology and profitability (ASIS, 2007; Hogan Lovells, 2010; USTR, 2012).

This point is underscored in a recent EC-sponsored survey of 537 businesses in Europe (EC, 2013). Among survey respondents, 75% ranked trade secrets as "strategically important to their company's growth, competitiveness and innovative performance." This reliance on trade secrets applied to firms of all sizes including small and medium size enterprises. The main reason cited by business (52%) for use of trade secrets over other forms of intellectual property protection was to avoid public disclosure of valuable information. In many countries, the relative ease of use and lack of registration requirements for trade secrets have led innovative small and medium size enterprises to rely on trade secrets as the default mode of intellectual property protection (Brant and Lohse, 2013). Moreover, unlike copyright or patent protection, trade secret law is not a particularly technical body of law.

The growing importance of trade secrets is underscored by recent government initiatives to improve protection. For example, in 2012, the European Commission released an indicative roadmap for an initiative to improve protection of trade secrets and confidential business information from misappropriation and misuse by third parties.[9] In 2013, the United States released the "Administration Strategy on Mitigating the Theft of US Trade Secrets", which included a set of action items for improved protection domestically and internationally.[10]

8 For example, barriers to accurate quantification include issues such as lack of internationally-standardised valuation methodology for undisclosed information and reluctance of many firms to identify publicly the value of their secret assets.

9 The roadmap is available on-line at the following location (as of 3 April 2013): http://ec.europa.eu/governance/impact/planned_ia/docs/2013_markt_002_trade_secrets_en.pdf.

10 This strategy is available on-line at the following location (as of 3 April 2013): http://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf.

Patent Versus Trade Secrets Protection

There is an extensive body of literature on the trade-offs between patents and trade secrets at both the institutional and firm level. Pooley (1997, 2012 update, pp. 32-40), for example, offers advice to firms wishing to protect their intellectual assets in which he highlights differences in protection between patents and trade secrets. He notes that often the nature of the asset provides a clear indication of the appropriate protection. Patents generally offer protection for specific technological inventions that are useful, novel and non-obvious. The patent process can be time consuming and expensive, requiring public disclosure of the idea. But, within the bounds of strictly defined claims, once a patent is issued, it offers the prospect of market exclusivity for a specific period. Trade secret protection is generally available for a broad range of commercial information that is useful and not widely known, but need not be novel. The broad scope covers subject matter that may not be patentable such as know-how. Provided appropriate efforts are made to ensure secrecy, trade secrets offer the possibility of protection without a limitation on duration, though not against independent discovery by a competitor or inadvertent disclosure by the owner.[11] Nonetheless, in many instances the innovators seeking protection for an idea face a choice in the type of protection they will seek.

The choice of protection can have social welfare implications. On the one hand, as Friedman et al. (1991) point out, patents offer the social welfare advantage of encouraging disclosure with all the positive spillover effects that may result. On the other hand, Cugno and Ottoz (2006) offer a model where trade secrecy is more socially optimal, because of the independent invention defence, which exists at all times with respect to a trade secret, but is either limited or non-existent in patent law.[12] As a result, trade secret owners may have fewer opportunities to charge supra-competitive prices.

The empirical literature shows that firms tend to rely heavily on trade secrets. Arundel (2001) found that European firms tended to prefer trade secrets to patents, with the preference more pronounced among smaller firms. Cohen et al. (2000) found similar results in a survey of US firms. An econometric study by Png (2012b) exploited variation among the laws of the US states and included construction of a simple index of trade secret protection. He found that between 1976 and 2006 US states that enacted trade secrets laws tended to experience increases in research and development expenditure (R&D) by high-tech and large manufacturing firms. At the same time, there was a tendency among such firms to reduce their reliance on patenting. Maskus (2012, p. 237) points out that trade secrets, in principle, can play an important role in developing countries where they offer a readily available form of protection for incremental innovation for which patents may not be available, financially viable or profit maximising.

11 Pooley (1997, 2012 update, p. 34) notes contrasts between patents and trade secrets with respect to subject matter, requirements, definition, disclosure, protection, duration, expense, risk and marketability. He also points out (ibid, p. 40) that depending on the nature of the innovation the choice between copyright and trade secret protection may be easier for innovators: copyright protects only the form of expression of your ideas, whereas trade secrets protection extends to the idea itself.

12 The United States recently incorporated a prior user rights defence into its patent law with the passage of the America Invents Act in 35 U.S.C. § 273, which may provide protection to independent inventors in certain, limited circumstances. However, independent invention after the date that a patent is filed never constitutes a defence.

4. Method

In order to pursue the economic analysis in the next phase of the present project, an indicator for the stringency of trade secrets protection is needed. The availability of such an indicator will permit comparisons of the stringency of trade secrets protection against relevant aspects of economic performance while controlling for other conditions. The strategy employed here is to take stock of the broad range of elements of legal protection for trade secrets, to consolidate this inventory into a list of elements that captures the key features of protection and that can generally be determined empirically, and then to compile an index based on these elements grouped into distinct components each representing a key aspect of protection. Rather than developing multiple indicators, a single index can offer the opportunity for various levels of analysis. The combined index score can be considered when an indicator of overall protection is appropriate or the index can be disaggregated into the key components for consideration of specific aspects of protection of trade secrets.

The analysis considers two sets of "elements" in order to gauge the variation in the available trade secrets protection and develop an index as a tool for use in the subsequent economic analysis. First, in order to determine the basic legal framework, the authors examined laws on the books and key cases that directly or indirectly relate to trade secret protection. This was done using the original laws, standard legal references and related expert commentary. Secondly, the functioning of the legal system was considered in relation to enforcement of trade secret protection in practice and in relation to alternative protection strategies. This was done via consideration of existing international indicators (e.g. available from World Economic Forum or Fraser Institute, among others), the academic literature, standard legal references and related expert commentary.[13]

The research design for this project presented a preliminary list of candidates for each of the two sets of elements. The elements were chosen for three reasons: (1) the presence or absence of these elements could allow one to make meaningful statements about the stringency of rights with respect to trade secrets; (2) they could represent significant differences among the laws of various countries; and (3) they may plausibly have marginal effects on the costs faced by firms (e.g. with respect to necessary secrecy measures) or their innovation-related decisions (e.g. regarding foreign direct investment (FDI) or resources devoted to research). Certain of these elements are referenced in the TRIPS Agreement, such as the protection of undisclosed pharmaceutical or agricultural chemical test data submitted in relation to marketing approval (Article 39.3).[14] However, it is not within the scope of this paper to draw any specific assessment with respect to the TRIPS Agreement.

---

13 Litigation statistics are not covered directly in the proposed assessment. This is in part due to lack of readily-available information for many countries. For example, while US legal records are searchable via systems such as Pacer or Lexis, the coverage of such systems varies significantly across countries around the world. Many countries do not have the capacity to provide ready on-line access to court case information. This would be a practical limit on the ability to ensure extensive geographic coverage for purposes of the present study. In addition, litigation statistics present difficulties in interpretation related to institutional context. For example, without additional contextual information, it may not be clear whether a low number of cases indicates that compliance is high, enforcement is lax or another factor is driving developments. Thus, such an assessment could prove resource intensive to implement. While in principle a review of legal case outcomes has the potential to yield new insights into court-related aspects of trade secret enforcement, such an approach was determined to exceed the scope of the present analysis.

14 The various elements of trade secrets protection retained for the present analysis are characterised individually and in combination. In the discussion and annexes for this report, data on the various

In implementing the research design, the preliminary list of elements was refined through an interactive process taking account of findings from our examination of the sample countries. The priority objective in this was to ensure coverage of key elements of the system of protection of trade secrets. Some new elements were added in this regard (e.g. with respect to availability of injunctions to eliminate wrongful head starts) and others were refined (e.g. the element for availability of emergency search to preserve and obtain proof was refined to take into account whether *ex parte* searches are available and who does them). Once coverage of key elements was ensured, a further consolidation of the elements was undertaken to avoid redundancy in the final set, to give particular focus to dimensions where there is variability between countries, and to ensure that internationally comparable information on the selected elements could be obtained via reasonable research efforts.

The research design takes the various legal means for protecting trade secrets and abstracts and generalizes them into a set of common, comparable elements. The resulting elements are still recognizable, meaningful and useful descriptions of legal provisions, but they are no longer bound to the context of a particular legal system. When the researchers examined a country's laws, they identified and isolated these elements regardless of labels – any law that directly[15] addresses trade secrets is covered, regardless of whether it explicitly mentions "trade secrets" or undisclosed information and whether it exclusively addresses trade secrets (in many cases, labor laws, tort laws, unfair competition laws, criminal codes, and procedural codes were all relevant). The research also identified these elements without regard to where they were found – it examined all legal methods for protecting trade secrets, such as statutory law, common law, administrative remedies, and laws of general application. The key consideration was identifying an objective indication of whether the element existed in a country's laws and how it was implemented.

The methodology employed here allows for effective cross-country comparisons despite considerable differences among legal systems. As a long-standing tradition of comparative law scholarship recognizes, it is possible to readily and clearly identify common points of law between countries despite very different legal systems.[16,17] The next section of this paper

elements are reported and may be employed for further analyses either separately or in various alternative combinations.

15 Laws that only incidentally sanction trade secret theft were not covered. For example, theft, breaking and entering, trespass, extortion, battery and other wrongful acts may be committed in the course of appropriating trade secrets, and various laws sanction such acts. However, such laws are only relevant where they sanction such acts *because* they involve trade secrets. For example, this project would not account for a law that imposes liability for the theft of a sheet of paper if that law does not address the existence or value of the trade secret printed on that piece of paper.

16 For example, common law jurisprudence may contain definitions and standards that are as clear, precise and well-established as those in civil codes. Courts in several common law countries consistently cite and apply a three factor definition of trade secrecy established in the English case of Coco v. A.N. Clark Eng'rs Ltd., [1969] RPC 41: "First, the information must itself … must 'have the necessary quality of confidence about it.' Secondly, that information must have been imparted in circumstances importing an obligation of confidence. Thirdly, there must be an unauthorised use of that information to the detriment of the party communicating it." See Annex 1 and Annex 2 of this paper for further details.

17 In another example, civil law systems may evolve approaches to a new problem as clearly and readily as do common law systems. For example, since 2000 French courts have increasingly extended the offense of "breach of trust" under Article 314-1 of the French Criminal Code to cover intangible information, thus allowing the prosecution of employees and others for trade secret misappropriation. See Christophe Garin, "Customer poaching can now be punished by criminal courts on the ground of breach of trust,"

surveys the situation for each country in the sample on the basis of the refined list of elements and considers similarities and points of divergence across the sample.

5. Survey of Legal Provisions and Practices

The results of the survey of legal provisions and practices are documented in *Annex 1: Country Charts and Preliminary Index Scoring*. The Annex presents results with respect to: source of law, definition and scope; covered acts; definition of duties and misappropriation; restrictions on liability; remedies; enforcement, investigation and discovery, and related regulations; and expert characterization of the operation of the system in practice.

The survey of legal provisions confirms that there is great variation among approaches to trade secret protection. The laws of various countries are harmonized at a high level of generality only. The following discussion briefly surveys similarities and differences among the trade secret laws of various countries.

5.1 Similarities Among Countries

As discussed in the Introduction, countries have similar definitions of trade secrecy due to the nature of trade secrets and the requirements of TRIPS. Beyond the similarities to the broad, three-part definition set forth in Article 39 of TRIPS, however, there are several other points of similarity among the trade secret laws of the countries surveyed in this paper.

- *Scope.* The scope of trade secret protection, while not the same in every country, follows certain well-defined categories. These categories are (1) technical information; (2) confidential business information; and (3) know-how. Technical information typically includes industrial processes, blueprints, formulae, and similar information regarding technology. Confidential business information typically includes customer lists (at least to the extent they include truly non-public information), financial information, business plans and similar information regarding the operation of a business. Know-how includes information about methods, steps and processes for achieving efficient results. Most countries recognise the first two categories (although they often treat them the same). Know-how is a term commonly used both in discussion of proprietary information and in agreements, but enjoys less formal recognition as a separate, defined category of trade secrets.

- *Defences.* Independent creation of a trade secret, where the defendant created a trade secret without access or reference to the plaintiff's trade secret, is explicitly or implicitly a universally recognized defence. Reverse engineering is also widely explicitly recognized as permissible and likely to be permissible in almost all cases.

- *Third Party Liability.* A third party that receives trade secrets with knowledge or reason to know that they were provided in violation of trade secret law is typically liable. Third parties that innocently and unknowingly receive trade secrets are less commonly liable, but they are still subject to injunctions in some jurisdictions.

- *Remedies.* Very broadly speaking, trade secret protection provides for civil remedies of injunctions and damages. However, this category is as much a source of variation as similarity and is thus discussed below. While the laws on the books provide for these remedies, they vary widely in specifics and practical availability.

Lexology (24 May 2012) at: http://www.lexology.com/library/detail.aspx?g=e11830fd-5222-4084-afdd-a160047f2fec . See Annex 2 of this paper for further details.

5.2 Key Points of Divergence

As foreshadowed above, the lack of a comprehensive international standard results in substantial variation among the legal systems with respect to trade secrets. The points of divergence are more numerous than the points of similarity. The following are key points of divergence among the laws of the countries studied:

- *Civil vs. Criminal.* A basic point of variation is whether a country protects trade secrets primarily through civil law, criminal law, or both – or, in some cases, administrative law.
- *Scope.* The most commonly protected category of trade secret is technical information. Most countries also protect confidential business information, and typically do not distinguish it from technical information. This equal treatment of technical information and confidential business information, however, does not necessarily prevail in every country.[18]
- *Duty.* Systems vary in how duties are imposed. In some instances, trade secret protection applies only where a defendant breaches a contractual or implied duty of confidentiality. In other instances, in addition to cases of breach of duty, trade secret law also applies where the secret was wrongfully obtained. In other instances, trade secrets are protected as intellectual property rights (IPRs). In those cases, the owner simply has exclusive rights to use them, without being required to show breach of duty or misappropriation, subject to the rights of others to independently develop or reverse engineer them.
- *Remedies.* Remedies vary widely in details and practical availability. One reason for the variance is that trade secret remedies tend to reflect national practice more than other intellectual property remedies, which have often been harmonized because of various international or transnational obligations, such as the European Union's Enforcement Directive. Thus, the types of damages available tend to depend largely on how the law of a particular country defines and awards damages. The availability of injunctive relief is partly a matter of national practice, but also a matter of the amount of proof required. Remedies such as seizure and return of materials are also typically matters of national law practice.
- *Evidence Gathering and Discovery.* Obtaining proof in trade secret cases is challenging. By their very nature, trade secrets constitute information that is not readily ascertainable and that can be hidden. Thus, evidence that a defendant has wrongfully obtained a trade secret may be similarly non-public and hidden. Moreover, a defendant may wish to keep trade secrets confidential for reasons other than legal liability – it too may wish to gain a commercial advantage against all competitors other than the original owner.

  For these reasons, proof of trade secret theft is often solely or largely in the possession of the defendant and closely guarded. There is some danger that the defendant can

[18] For example, specific provisions of French criminal law sanction the disclosure of technical information by employees and managers, but not confidential business information. However, in recent years generally-applicable provisions of French criminal law have been used to prosecute the disclosure and misappropriation of confidential business information, so the distinction may be fading in this particular instance.

effectively destroy such evidence if it becomes aware of a lawsuit. It also may be necessary to conduct an in-depth investigation to determine what was taken, how it was taken, by whom, and what has been done with it. These issues may not be readily apparent from easily accessible sources. It thus may be difficult to build a case without assembling documents, physical evidence, and conducting interviews.

Various references in the literature indicate that the ability to gather evidence in a trade secret case is crucial. Yet, the approaches vary widely among countries. This variation is largely a matter of national procedural law and practice in civil cases generally. On one end of the spectrum of discovery laws and practice is the United States, with its very broad disclosure rules and practice. These rules and practices make it easier to prove a case, but are often criticized as greatly increasing the expense and duration of litigation. Toward the other end of the spectrum are many civil law countries, where pre-trial discovery is limited, typically confined to documentary evidence, and done under the direct supervision of the court. At the furthest end of the spectrum may be China, which has extremely limited discovery, but where, according to experts, courts prefer original, documentary evidence to prove a case, which is very difficult to obtain without extensive discovery.

Another point of variation in evidence gathering rules and practices is the availability of a preliminary, emergency action to preserve proof. Many, but not all, countries have emergency, pre-trial procedures to preserve evidence. In their broadest forms, these procedures (often called "Anton Piller" orders after the English case from which many common law countries take their procedure) allow a party to obtain ex parte approval to conduct a search of a prospective (i.e. before a case begins) defendant's premises and to seize relevant evidence.

Under the broadest form of this procedure, available in a limited number of countries, a plaintiff may obtain a search on an ex parte basis and send a representative to direct the search. Plaintiffs in trade secret cases value these features, as the lack of advance warning prevents a prospective defendant from concealing evidence. Also, the presence of plaintiff's representative at the search makes it much more likely that the search finds relevant evidence because of the plaintiff's expertise and detailed knowledge of the trade secret. However, these features are not available in most countries surveyed. In fact, several countries have no preliminary search procedure at all.

While the interest of a plaintiff in securing evidence may be key to many trade secret cases, several jurisdictions have moved to balance plaintiffs' needs against defendants' rights. The experience of the United Kingdom and other jurisdictions has raised concerns that a plaintiff may, ironically, use preliminary procedures to misappropriate a defendant's secrets or interfere with its business (Andrews, 1987). Thus, authorities have clarified that courts should not grant such orders routinely. For example, the Chief Justice of the Australian Federal Court issued "Federal Court Practice Note No. 24—Search Orders (also known as "Anton Piller Orders")" (5 May 2006) to curb perceived abuses of such orders.

- *Duty of Employees.* Employees are typically, but not everywhere, under an implied duty of confidentiality during the term of employment. Express agreements to keep information confidential are enforceable during the term of employment. There is wide variation as to what an employee's duties are after termination of employment. Some jurisdictions will continue to impose an implied duty after the end of

employment, but many will not. Many restrict enforcement of express contracts for confidentiality after employment as well. A typical restriction on both express and implied duties is that they do not apply to general skills and knowledge and cannot interfere with the employee's ability to make a living.

- *Non-Compete Agreements.* The enforceability of post-employment non-competition agreements varies widely.[19] Such is also the case with non-competition agreements between commercial entities. Most typically, they are enforceable only if reasonable with respect to duration and geographic scope. However, stricter regulation of enforceability, length, and scope is also the rule in some countries. Non-compete agreements between commercial entities are also subject to competition law. This paper does not address competition regulation, as it does not appear to affect trade secret protection uniquely, but rather applies to commercial agreements generally.

- *Protection of Secrets During Litigation.* Trade secret litigation may expose the plaintiff's confidential information to security risks. First, the plaintiff needs to prove the existence of a trade secret. The evidence submitted may expose the secret. Second, proving that the defendant possesses the trade secret may require putting evidence on the record that further exposes the secret. Finally, the court may need to discuss aspects of the secret in its orders and opinions.

  Laws and procedures can mitigate these risks from litigation. A court may hold hearings "in camera"—closed hearings open only to the parties, typically. The court may seal the record, thus blocking public access to it. The court might also physically secure evidence, such as by locking it in a safe. It may also restrict the access of the defendant and its personnel and agents to trade secrets (e.g., access might be limited to the lawyers on the case). Finally, a court may redact portions of its published opinions or choose not to publish the opinion at all.

  From the commentary in the literature, it appears that the availability of these measures greatly affects the risk in bringing a trade secret action. Without sufficient protection, a lawsuit could leave a plaintiff worse off. A defendant may actually guard a trade secret, as it may confer an advantage over the defendant's and plaintiff's mutual competitors. Thus, the prospect of a trade secret lawsuit in a country with insecure court procedures could require a choice between not filing a suit and allowing a single competitor to exploit one's secret, and filing a suit and exposing the secret to all competitors.

  Although litigation security measures appear important to effective trade secret protection, there is wide variation in the availability and effectiveness of such measures among countries. Some countries routinely provide in camera hearings, while others do not. There is also variation with respect to whether defendant and all of its agents have full access to the record.

- *Data Exclusivity.* Data exclusivity is a form of protection related to trade secret law. Data exclusivity provisions govern the use of data submitted for regulatory approval of chemicals – particularly pharmaceuticals and agricultural chemicals. There is a

[19] The OECD has also considered this issue in the context of knowledge networks and markets. For example, a paper on *Knowledge Flows and the Mobility of Skilled Employees: An International Perspective on the Role of Non-Compete Agreements and their Legal Enforcement* examined these issues in 2012 [DSTI/EAS/STP/NESTI/TIP(2012)10, Fernando Galindo-Rueda].

wide variance among countries in how they implement these regimes. Most countries reviewed in this paper protect test data for new chemical entities from disclosure or from use by competitors seeking regulatory approval for their own products for a term of years after regulatory approval. The term of years varies widely. Some countries also protect data submitted to obtain approval for new uses (as opposed to entirely new products), but many do not.

- *Technology Transfer Regulations.* In the 1960s and 1970s, many countries adopted technology transfer laws regulating inbound technology licenses.[20] These laws were intended to ensure that foreign investors transferred know how to local enterprises and workers. They typically required registration of agreements and often gave regulatory agencies the power to disapprove substantive terms that interfered with technology transfer. Such provisions often affected trade secrets. For example, some provisions prohibited indefinite length confidentiality provisions. Others prohibited provisions that restricted the use of trade secrets after the expiration of the agreement or that required return of materials containing trade secrets.

This review highlights a number of fields of law as they relate to trade secrets protection. From this, it appears that *general legal system quality* may be particularly relevant in the case of trade secret protection across the countries surveyed. Although the quality of the legal systems varies widely between countries, it is a characteristic that plays an important role in trade secret protection. First, protection of trade secrets is often put into practice through generally applicable causes of action such as contract enforcement, labor law or tort actions. Reliable enforcement of contracts and property rights and the impartiality of the courts are thus important to a trade secret regime. Second, trade secret owners are particularly dependent on recourse to courts in the event of an appropriation because of the great vulnerability of trade secrets. Once widely disclosed, they are extinguished. Thus, a prospective developer or owner of a trade secret must be cognizant of how swift, reliable and predictable the courts are in case its own attempts to maintain secrecy are breached.

5.3 A Deeper Look at Countries in the Survey

The foregoing comparison based on the Annex 1 charts highlights the substantial diversity among the survey countries. In order to consider the origins of this diversity and its impact on the operations of the legal systems for protection of trade secrets, a more detailed examination is carried out for the BRICS and OECD countries. This is presented in Annex 2: *Detailed Overviews for the BRICS and a Sample of OECD Countries*. The narrative discussions in Annex 2 serve to give a rich and full sense of the issues that trade secret protection addresses and the common and diverse ways in which countries address them.

Based on the international comparisons in Annex 2, a hierarchy of trade secret challenges emerges which might be characterised as follows:

- *"Ordinary" Trade Secret Appropriation*. These problems result from departing employees or business partners taking information or from opportunistic competitors seizing an opportunity to illicitly obtain information.

[20] For a comprehensive, recent review of these laws, see Padmashree Gehl Sampath and Pedro Roffe, "Unpacking the International Technology Transfer Debate: Fifty Years and Beyond," *ICTSD Working Paper* (June 2012), available at: http://ictsd.org/downloads/2012/07/unpacking-the-international-technology-transfer-debate-fifty-years-and-beyond.pdf (as of 15 August 2013).

- *Corporate Espionage*. These problems result from more systematic schemes by competitors to infiltrate a competitor's operations through such actions as planting employees, bribery or extensive infiltration of computer systems or electronic eavesdropping.
- *State Sponsored Corporate Espionage.* Increasingly, some governments are expressing grave concerns regarding government-sponsored systematic schemes to appropriate trade secrets.

Ordinary trade secret appropriation is typically addressed through civil enforcement. Evidence of the wrong is often in the possession of the trade secret owner or relatively easy to obtain. The laws of the countries surveyed all address the problem of departing employees and other parties who appropriate trade secrets by breaching contracts or other duties. This issue is typically addressed through a variety of means – trade secret law, breach of contract, and/or labor law. There is greater divergence in addressing the opportunistic behavior of parties who do not have a prior relationship with the trade secret owner. Most typically, the law addresses such actions as misappropriation. Not all countries recognize an action for misappropriation. For example, common law jurisdictions take a relationship-based view of trade secrecy, and thus some, for example New Zealand and India, do not recognize a civil action for misappropriation.

The challenge of corporate espionage highlights the importance of criminal law for addressing difficult problems of gathering evidence. A much smaller number of countries in the sample offer criminal remedies. As the narratives show, where available, criminal law offers useful investigative tools against systematic espionage such as "sting" operations and large-scale, long-term operations that are beyond the means and authority of individual trade secret owners. In some jurisdictions, such as Germany, criminal remedies play an important role in supplementing the limited discovery available in civil cases.

Another point that emerges from the narratives in Annex 2 is that the stringency of trade secret protection in countries with relatively well-developed statutory protections can be undermined by specific requirements and implementation factors. For example, China and Russia have fairly well-defined legal protections, but the stringency of those protections is partly offset by weaknesses in implementation and additional, unusual evidentiary requirements. In other countries, including Brazil, stringency of the laws on the books is sometimes inconsistent with the approaches used in specific areas such as technology transfer or data exclusivity.

6. Trade Secret Protection Index

From the foregoing discussion, it is clear that there is significant variation in the available protection for trade secrets across this diverse sample of countries. Phase II of this project anticipates consideration of the relevance of such variation for certain aspects of economic performance, particularly those related to innovation.[21] As noted above, in order to conduct a quantitative assessment of the relationship, it is useful to have an indicator for the stringency of available trade secrets protection. This section presents a preliminary version of an indicator developed for this purpose: the Trade Secrets Protection Index (TSPI).

[21] The two phases of the project correspond to the two papers foreseen in the research design as deliverables.

The development of the TSPI proceeded based on several considerations. First, five components were designated as representing key aspects of protection of trade secrets that also emphasize features where there is some variation across countries that may influence the stringency of protection. Second, the relevant entries from the refined list of elements (i.e. from Annex 1) were grouped under the appropriate component heading. The elements were phrased to enable scoring based primarily on objective criteria, supplemented in some cases by qualitative information as necessary (e.g. in certain areas related to system operation). Third, in order to ensure coherence across the components, the authors opted for an integrated index approach rather than multiple indicators. (The TSPI can be disaggregated into its components if a focus on certain aspects is helpful for a particular discussion.) Fourth, the index was designed to emphasize transparency with scores supported by a text chart for each country and verifiable references. Fifth, the index is designed to provide an indication of the stringency of available protection; it aims to be neutral in this assessment. In other words, a higher or low score reflects the strength of protection and not an assessment of the appropriate level of protection.

It bears emphasis that the index's function is descriptive, not normative, and the scores it produces are thus neither grades nor ratings. Rather, the score is strictly a measure of stringency of protection. As a measurement tool, the TSPI simply measures. Additional empirical work or subjective assessment will determine whether a particular measurement is associated with particular outcomes or should be assigned a particular adjective.[22]

The initial implementation of the TSPI is for a single time period for the sample countries. Econometrically, this will permit cross-sectional analysis. However, in future, subject to available resources, the index could be deepened to include multiple time periods and additional countries. This would permit use of more powerful econometric techniques for dynamic assessments based on panel data for a broader set of countries. Moreover, the dynamics of the protection for trade secrets could be compared with those for protection of other types of intellectual property (e.g. patents) in order to gain a more integrated view of their effects.

The development of this index is a pioneering effort in the analysis of protection of trade secrets. However, it should be noted that a variety of similar indices exist in the literature covering various types of intellectual property. For example, Ginarte and Park (1997) and Park (2008) employed laws-on-the-books approaches to examine protection of patents, trademarks and copyright. Also, the Fraser Institute (2012) and World Economic Forum (2012), among others, have developed substantial sets of relevant systemic indicators for use in economic analyses. Such indicators have been utilized in a number of studies conducted by the Working Party of the Trade Committee and other parts of OECD.[23]

22 The index avoids summative descriptive assessments such as whether protection is "comprehensive" or "well-established." The accumulation of elements and the resulting score speaks to such issues more precisely than any subjective assessment, and does so in a replicable, generalizable manner.

23 Several Trade Committee studies considered policies for protection of intellectual property rights in relation to relevant economic performance indicators. OLIS references include: TD/TC/WP(2003)10/FINAL, TD/TC/WP(2004)31/FINAL, TAD/TC/WP(2007)19/FINAL and TAD/TC/WP(2010)12/FINAL. Subsequent OECD *Trade Policy Working Papers* were published as: Park and Lippoldt (2003); Park and Lippoldt (2005); Park and Lippoldt (2008); and Cavazos, Lippoldt and Senft (2010).

6.1 Index Composition

Chart 1 presents the detailed composition of the index and its scoring. The index is structured around five main components:

1. Definitions and coverage
2. Specific duties and misappropriation
3. Remedies and restrictions on liability
4. Enforcement, investigation & discovery; data exclusivity
5. System functioning and related regulation

The approach to scoring provides up to one point for each of the five main components of the index and a maximum total score for the index of five points. However, as can be seen in the Chart, the number of elements covered by each of the main components of the index varies widely. For example, the definition and coverage of trade secrets protection comprises 12 elements, whereas the system functioning and related regulation comprises 4 elements. In order to maintain balance across the five components of the index, the scoring for the various elements under each of the five main components was normalized to ensure equal weighting. In other words, the elements for each main component add up to a maximum score of one.[24]

6.2 TSPI - Index Results

Table 1 presents the total scores by country according to various weighting schemes. The three weighting schemes are:

1. Equal weights across the components (20% each x 5);
2. 40% for Enforcement, investigation & discovery; data exclusivity and 60% split evenly among the other components; and
3. 40% Remedies and restrictions on liability and 60% split evenly among the other components.

Interestingly, the three weighting schemes yield similar country rankings as shown by the high scores for the Spearman rank correlation coefficients in the table. In other words, according to this indicator, the use of alternative weighting schemes does not substantially change the country rankings. Thus, in the absence of a compelling rationale for unequal weights, the authors have opted to employ equal weights.[25]

Under the equal weights approach, the scores range from a low of 2.52 (China) to a high of 4.57 (United States). Figure 1 provides an overview of the scores across the countries covered in the sample for each of the TSPI components and for the TSPI as a whole. The OECD

[24] For example, component 4 *Enforcement, investigation and discovery; data exclusivity* is comprised of six elements. The value for the component 4 score can range from 0 to one. In the final calculation of the score for the overall component, the scores for any given element would be no more than 1/6 of one point. This would be the case, for example, for data exclusivity for drugs or data exclusivity for agricultural chemicals (each would contribute no more than 1/6 of one point to the component score).

[25] A similar weighting approach and rational was employed by Ginarte and Park in developing their widely-cited Patent Rights Index. See Ginarte and Park (1997, pp. 288-89) for their discussion of weighting considerations.

countries tend to have relatively high total scores, though partner countries such as Singapore and Malaysia have scores falling within the OECD range. Other developing countries, including Brazil and South Africa, deliver total scores above 3.0. However, three countries at the bottom of the range have total scores below 3.0: China, Russian Federation and India.

A review of the scores for the individual components of the index reveals different country rankings for each component, reflecting the variation in the manner countries construct and operate their trade secrets regimes. In particular, the component for "System functioning and related regulation" reveals a different mix of countries near the top of the rankings than for the total. For example, Sweden emerges as having the highest score among the European nations, whereas for some other components it ranks closer to the average scores. For certain other individual components of the index, countries such as Brazil, Bulgaria, Colombia, Russia and Singapore appear among the top 5 or 6 countries in the rankings. With the exception of Singapore, however, the total scores for these countries fall outside of the range for OECD country scores. This reflects weakness in their scores for certain other components of the TSPI.

Table 2 and Figure 2 present the summary results for each country in the sample including the overall total score and the sub-totals by index component, as well as the averages by component. Figure 2 highlights in a visual manner, the contributions of each component to each country's total score. The breakdown by component reflects the particularly low scores for Brazil, China, India and the Russian Federation with respect to system functioning and related regulation. This highlights implementation challenges faced by these countries. A number of OECD countries, as well as Singapore and South Africa, delivered relatively stringent protections in the handling of duties and misappropriation related to trade secrets. The United States' high score was reinforced in part by relative strengths in the components referring to remedies and enforcement and related provisions.[26]

The variation in the component scores highlights the different combinations of legal provisions and practices that countries exhibit to arrive at a given TSPI total score. The Spearman rank correlation is relatively high (0.853) between the scores for overall system functioning and the TSPI total scores. The Spearman rank correlation is also relatively high (0.720) between the scores for the component "specific duties and misappropriation" and the TSPI total scores. That is, country rankings are relatively consistent in the scores for these two components and the TSPI total scores. However, the country rankings vary significantly with respect to the other three components relative to their total scores. For example, a country without criminal statutes addressing trade secrets may have a low score in remedies, but strong scores for "specific duties and misappropriation" and "enforcement, investigation and coverage" and a relatively high TSPI total score. Another country, may have a similar TSPI total score, but arrive at that level via a higher score in "remedies and restrictions on liability" due in part to having criminal statutes addressing trade secrets.

7. Conclusions

Anchored by a review of a broad sample of countries, this international comparative examination of protection of trade secrets highlights the role played by the TRIPS Agreement Article 39 in orienting WTO Member countries in the basic definition and scope of trade

[26] Annex Table A1 (Annex 1) provides the detailed scoring for each element and component of the index for each country. In the event a user would like to consider alternative approaches to constructing indicators, these data will provide the essential building blocks (e.g., for recombining various elements or reweighting the components).

secrets. At the same time it underscores the wide range of approaches employed by the sample countries in the implementation of their TRIPS obligations with respect to protection of trade secrets. This conclusion is supported by a structured empirical assessment of the legal regimes in the sample countries. One important contribution of this paper is the presentation of the underlying information in Annexes 1 and 2, and the taxonomy of trade secrets these materials embody. The charts and taxonomy provide a clear, objective point-by-point basis for making comparisons among countries.

From the review of the sample countries, some specific areas of divergence can be identified. For example, differences exist with respect to gathering of evidence, protection of trade secrets during litigation, technology transfer and effectiveness of enforcement via the legal systems. With respect to the procedures available for gathering evidence, some jurisdictions provide for emergency actions to preserve proof, but many do not. Furthermore, no two systems of discovery are quite the same, and many are quite weak. The ability to protect secrets during litigation also varies substantially between countries. Some developing countries, including several BRICS, have laws intended to facilitate technology transfer, which in some cases may cut across certain aspects of the ability to protect trade secrets. Moreover, across the sample of countries, variation in the effectiveness of the legal systems is likely to have significant effects on enforcement. Such diversity in protection of trade secrets can be reasonably expected to influence firm-level decision-making.

In anticipation of subsequent analysis in the next phase of the project (Box 4), this paper presents a preliminary indicator for assessing the stringency of available protection: The Trade Secrets Protection Index (TSPI). The diversity of approaches to protection in trade secrets across the sample countries are reflected in the scores for the TSPI, indicating that the stringency of protection for trade secrets also varies. This variation may matter materially for the operation of firms and, hence, may influence certain aspects of economic performance (in particular, in relation to innovation), topics that will be considered in the coming economic analysis.

Box 4. Phase 2 of the Project: The Economic Assessment of Trade Secret Protection

As foreseen in the scoping paper, the next phase of the trade secrets project will focus on economic analysis. It will be based on dual approaches: a qualitative assessment and a quantitative assessment. The objective will be to examine empirically the relationship between the stringency of protection for trade secrets and performance in the types of economic indicators that may be responsive to variation in protection of trade secrets.

The qualitative assessment will begin with a brief review of the economic and business literature and available statistics to describe the theoretical and perceived role of trade secrets in economic performance and innovation. Information on firm-level impacts will be included, including with respect to small and medium size firms (SMEs) and start-ups. The relationship to national economic development will be considered. Where possible, the project will highlight evidence on the value of trade secrets, as well as the scope and nature of trade secret theft and misappropriation among competing firms.

The quantitative assessment will consist of two elements:

Expanded coverage for the Trade Secret Protection Index: Building on the preliminary TSPI from the background paper, this element will present expanded results for the TSPI including any revisions as well as coverage of additional countries and one or more additional time periods. Basic sample statistics for the dataset will be presented. The aspects of protection contributing to variation in scores will be highlighted. The relationship between stringency of protection and country features will be considered. For example, relationships to geography, level of development or organizational affiliation could be considered. The analysis will consist of narrative descriptions supported by presentation of the results in summary tables, simple cross-tabulations, or graphical presentations of the results (e.g. results by country grouping).

Assessment of trade secret protection in relationship to relevant economic performance indicators: Using standard economic methods, the relationship of the national-level trade secrets protection to relevant economic performance indicators (at national, sectoral or firm-level) will be considered. The modelling will be based on standard regression analysis.[27] The selection of economic indicators will emphasize types of activity where effective protection of trade secrets may be reasonably hypothesized to play a role in promoting expanded activity. For example, such protection may be hypothesized to be a factor influencing R&D expenditure, FDI, or trade in certain sectors. Where regression analysis is pursued, particular attention will be focused on issues of correlation among the independent variables and of endogeneity.[28]

The conclusions will highlight empirical findings with respect to the importance of protection of trade secrets for relevant indicators of economic performance. If the data permit, various dimensions of trade secret protection (e.g. including legal framework and implementation issues related to enforcement) will be considered independently in relation to the various aspects of economic performance. While policy prescriptions will be avoided, the conclusions will present policy-relevant findings based on the actual experience with trade secrets protection. Such an assessment may help policy-makers in the identification of policy options for improved economic performance with respect to trade secrets.

27 The approach for the economic assessment will be similar to that from previous studies under the Working Party of the Trade Committee on patents, copyright and trademarks. These studies considered policies for IPR protection in relation to relevant economic performance indicators. References include: TD/TC/WP(2003)10/FINAL, TD/TC/WP(2004)31/FINAL, TAD/TC/WP(2007)19/FINAL and TAD/TC/WP(2010)12/FINAL and OECD *Trade Policy Working Papers*: Park and Lippoldt, 2003; Park and Lippoldt, 2005; Park and Lippoldt, 2008; and Cavazos, Lippoldt and Senft, 2010.

28 With respect to endogeneity, there are a few technical options that may be available to address this, if necessary. One option is to lag time series by one or more periods.

Chart 1. Trade Secrets Protection Index

Components and scoring	Score range	Normalised score
1. Definition and Coverage	**0-12**	**0-1**
a) Scope		
• If scope covers all confidential business information, subject to: 1) deriving value from secrecy and 2) the owner's reasonable efforts to maintain secrecy, score = 1; If scope also subject to requirement that information is imparted to the recipient in confidence, score = ½	0,1	
b) Additional Elements of Definition		
• Inventory of trade secrets required (requirement=0; no requirement=1)	0,1	
• Must be reduced to writing (requirement=0; no requirement=1)	0,1	
• Must be identified as a trade secret to recipient (requirement=0; no requirement=1)	0,1	
• Written notice to recipient required (requirement=0; no requirement=1)	0,1	
c) Acts covered as civil infringement:		
• Breach of duty (not covered=0, partially covered=½[29], covered=1)	0,1	
• Wrongful acquisition or misappropriation (not covered=0, covered=1)	0,1	
• Third party liability for acquisition with knowledge or reason to know (not available=0, available=1)	0,1	
• Third party liability for acquisition without knowledge - enjoin "innocent parties" (not available=0, available=1)	0,1	
d) Acts covered by criminal law		
• Breach of duty (not covered=0, partially covered=½, covered=1)	0,1	
• Wrongful acquisition or misappropriation (not covered=0, covered=1)	0,1	
• Third party liability for acquisition with knowledge or reason to know (not available=0, available=1)	0,1	
• Third party liability for acquisition without knowledge, enjoin "innocent parties" (not available=0, available=1)	0,1	

29 E.g. the duty of confidentiality might be imposed on employees, fiduciaries and third parties with access to information. Partial coverage might arise if under a country's legal regime licensees cannot be covered.

Chart 1. Trade Secrets Protection Index (continued)

Components and scoring	Score range	Normalised score
2. Specific duties and misappropriation[30]	**0-5**	**0-1**
• Commercial relationship (covered if arising from: express agreement ½ + implied duty ½)	0,1	
• Current employment relationship (covered if arising from: express agreement ½ + implied duty ½)	0,1	
• Past employment relationship (covered if arising from: express agreement ½ + implied duty ½)	0,1	
• Restrictions on post-relationship duty of confidentiality (if any restrictions on matters beyond general skills and knowledge, by relationship: commercial ½ + employment ½)	0,1	
• Validity of contractual restrictions on competition (if unenforceable=0, significant limitations=½ (e.g., limited by time or place for either commercial or post-employment situations), generally enforceable=1)	0,1	
3. Remedies and Restrictions on liability	**0-11**	**0-1**
a) Restrictions on liability		
• Additional elements of proof in infringement claims (if none: civil=½ + criminal=½, criminal ½ point; score 1 if there no criminal law and civil score is ½)	0,1	
b) Civil remedies		
• Preliminary injunction (if available = 1, if not = 0)	0,1	
• Ex parte action available under preliminary injunction (if available = 1, if not = 0)	0,1	
• Permanent injunction (if available = 1, if not = 0)	0,1	
• Injunction to eliminate wrongful head start (if available = 1, if not = 0)	0,1	
• Delivery or destruction of infringing materials (if available = 1, if not = 0)	0,1	
• Compensatory damages (direct or out of pocket damages or consideration of profits or other damages= 1)	0,1	
• Yielding of defendant's profits (if available = 1, if not = 0)	0,1	
• Availability of punitive or statutory damages (if available = 1, if not = 0)	0,1	
c) Criminal remedies		
• Fines, damages or loss of assets (if not available = 0, if minimal per expert opinion= ½, if substantial = 1)	0,1	
• Jail sentence (if available = 1, if not = 0)	0,1	

30 The treatment of duties is split within this framework. General coverage of duties is scored under index component 1 (Definitions & Coverage). Component 2 responds to the availability of recourse for specific duties. This permits a detailed assessment, ensuring the indicator responds to variation in key elements.

Chart 1. Trade Secrets Protection Index (continued)

Components and scoring	Score range	Normalised score
4. Enforcement, investigation and discovery; data exclusivity	**0-6**	**0-1**
a) Enforcement, investigation and discovery		
• Emergency search to preserve and obtain proof (unavailable=0, available but with significant restrictions= ½ (e.g., conducted solely by an official or 3rd party expert), readily available=1)	0,1	
• Ex parte emergency search availability (unavailable=0, available but with significant restrictions=½, readily available=1)	0,1	
• Pre-trial discovery (unavailable=0, documentary only or strict limitations = ½, ready availability of documentary and interrogatories = 1)	0,1	
• Protection of confidentiality of trade secrets in litigation (none=0, partial= ½, fully available=1)	0,1	
b) Data exclusivity		
• Drugs (years: 0=0; 0.1-3=1/3; 3.1-7.9=2/3; >8=1)	0,1	
• Agricultural chemicals (years: 0=0, 0.1-4.9=1/3, 5-8=2/3; > 8=1)	0,1	
5. System functioning and related regulation	**0-4**	**0-1**
• Technology transfer: registration requirement (none=1; one or more = 0)	0,1	
• Technology transfer: substantive review or regulation (none=1; one or more = 0)	0,1	
• Fraser Institute score for *Legal System and Security of Property* Rights (score ranging from 0 to 10, divided by 10)[31]	0,1	
• Expert characterisation of the operation of the protection in practice (NB, based on internationally recognised or peer-reviewed sources; see country charts for details) (Negative = 0; none = ½; positive = 1)	0,1	
		======
Index Total		**0-5**

31 The Fraser Institute (2012, pp. 3 and 273-5) score for *Legal System and Security of Property Rights* is a composite indicator produced annually. Scores can range from 0 to 10. Based on objective indicators and expert assessments, it takes into account judicial independence, impartiality of courts, protection of property rights, military interference in the rule of law and politics, integrity of the legal system, legal enforcement of contracts, regulatory restrictions on the sale of real property, reliability of the police and business costs of crime. For details see Annex 1 of the present report and http://www.freetheworld.com/reports.html .

Figure 1. Trade Secrets Protection Index and Component Scores, by country, 2010

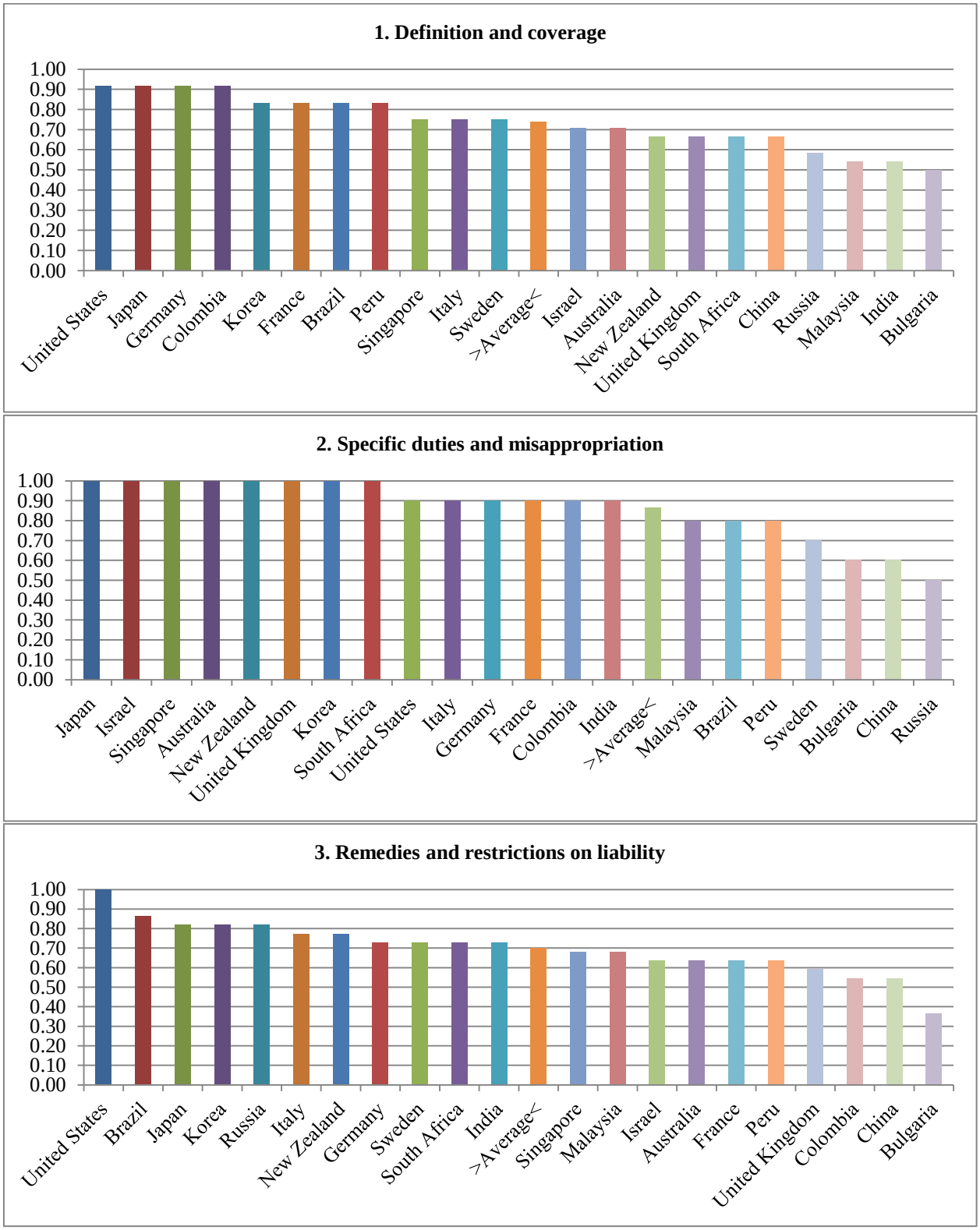

Figure 1. Trade Secrets Protection Index and Component Scores, by country, 2010 (continued)

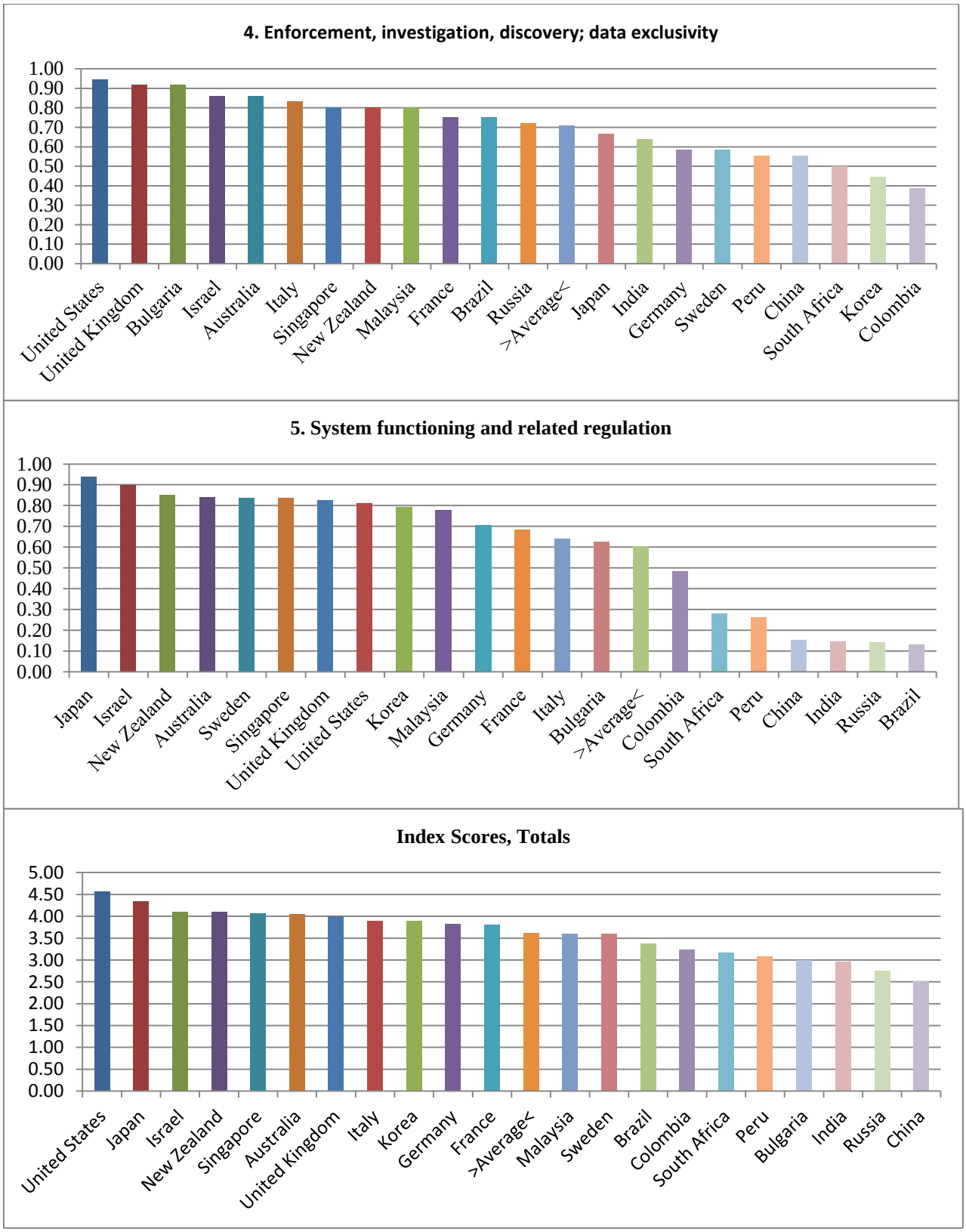

Figure 2. Trade Secrets Protection Index, by component and country, 2010

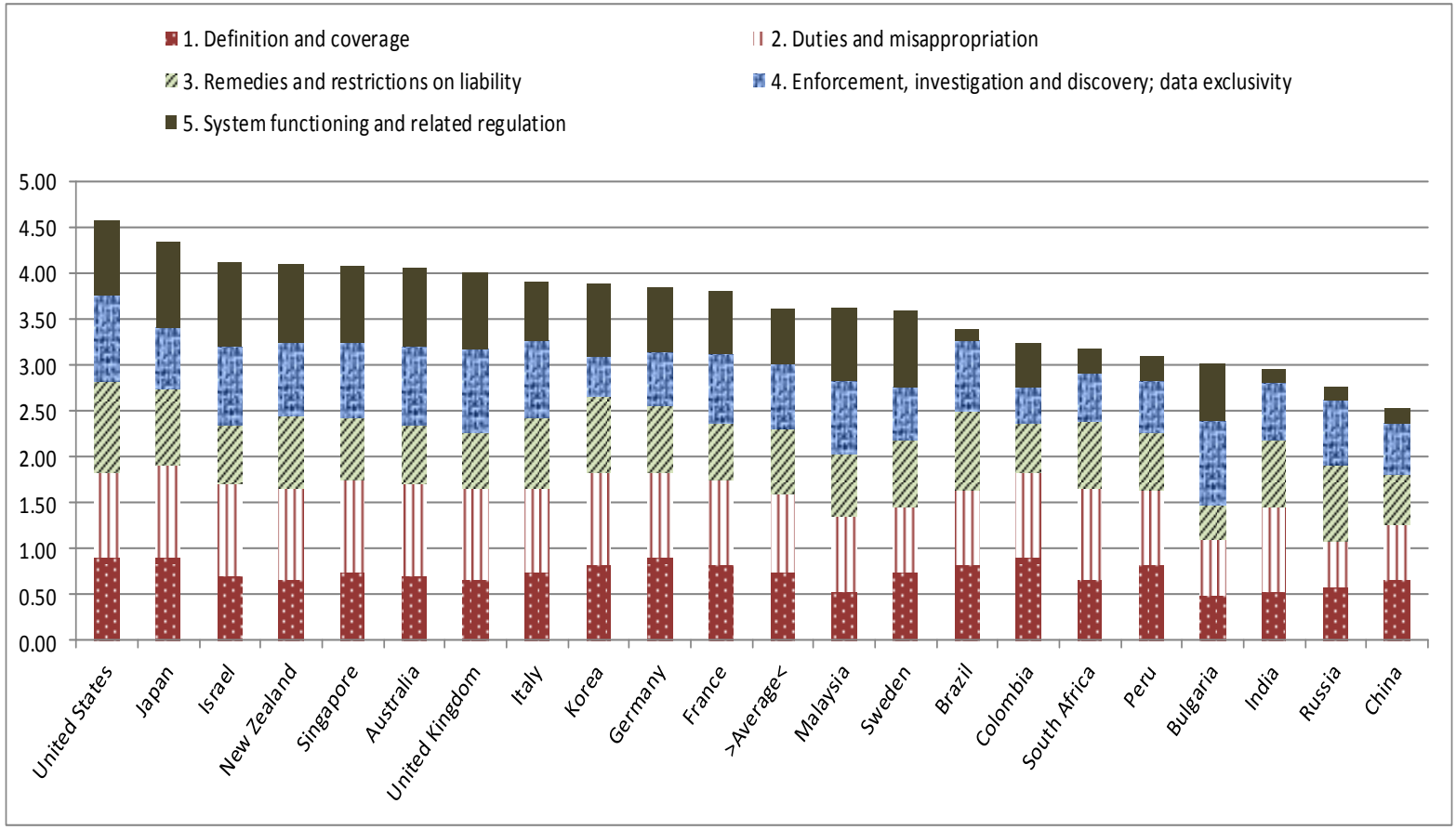

Table 1. Trade Secret Protection Index, Statistics and Total Scores, Alternate Weights, 2010

Country	**Total Scores, by weighting scheme**		
	Equal weights; 20% for each component	40% for Enforcement, investigation & discovery; data exclusivity; 60% divided equally among the other components	40% for Remedies and restrictions on liability; 60% divided equally among the other components
Australia	4.05	4.11	3.83
Brazil	3.38	3.47	3.61
Bulgaria	3.01	3.40	2.71
China	2.52	2.58	2.57
Colombia	3.23	2.91	3.11
France	3.80	3.79	3.65
Germany	3.83	3.60	3.78
India	2.95	3.01	3.13
Israel	4.10	4.15	3.87
Italy	3.90	3.97	3.89
Japan	4.34	4.09	4.28
Korea	3.89	3.47	3.94
Malaysia	3.61	3.71	3.56
New Zealand	4.09	4.07	4.04
Peru	3.09	3.01	3.11
Russian Federation	2.76	2.97	3.10
Singapore	4.07	4.06	3.90
South Africa	3.18	3.01	3.29
Sweden	3.60	3.43	3.61
United Kingdom	4.00	4.15	3.74
United States	4.57	4.61	4.68
Average Score	3.62	3.60	3.59
Max	4.57	4.61	4.68
Median	3.80	3.60	3.65
Min	2.52	2.58	2.57
Standard Deviation	0.55	0.54	0.51
Coefficient of Variation	0.15	0.15	0.14
Correlation Coefficient (equal weight scores versus alternate schemes)		0.940	0.955
Spearman Rank Correlation (equal weight ranking versus alternate schemes)		0.932	0.940

Table 2. Trade Secrets Protection Index, by country and index component, 2010

Components and scoring	Score range	Australia	Brazil	Bulgaria	China	Colombia	France	Germany	India	Israel	Italy	Japan
1. Definition and coverage	0-1	0.71	0.83	0.50	0.67	0.92	0.83	0.92	0.54	0.71	0.75	0.92
2. Specific duties and misappropriation	0-1	1.00	0.80	0.60	0.60	0.90	0.90	0.90	0.90	1.00	0.90	1.00
3. Remedies and restrictions on liability	0-1	0.64	0.86	0.36	0.55	0.55	0.64	0.73	0.73	0.64	0.77	0.82
4. Enforcement, investigation & discovery; data exclusivity	0-1	0.86	0.75	0.92	0.55	0.39	0.75	0.58	0.64	0.86	0.83	0.67
5. System functioning and related regulation	0-1	0.84	0.13	0.63	0.16	0.49	0.68	0.71	0.15	0.90	0.64	0.94
Totals	**0-5**	**4.05**	**3.38**	**3.01**	**2.52**	**3.23**	**3.80**	**3.83**	**2.95**	**4.10**	**3.90**	**4.34**

Components and scoring	Score range	Korea	Malaysia	New Zealand	Peru	Russia	Singapore	South Africa	Sweden	United Kingdom	United States	Average
1. Definition and coverage	0-1	0.83	0.54	0.67	0.83	0.58	0.75	0.67	0.75	0.67	0.92	0.74
2. Specific duties and misappropriation	0-1	1.00	0.80	1.00	0.80	0.50	1.00	1.00	0.70	1.00	0.90	0.87
3. Remedies and restrictions on liability	0-1	0.82	0.68	0.77	0.64	0.82	0.68	0.73	0.73	0.59	1.00	0.70
4. Enforcement, investigation & discovery; data exclusivity	0-1	0.44	0.80	0.80	0.55	0.72	0.80	0.50	0.58	0.92	0.94	0.71
5. System functioning and related regulation	0-1	0.80	0.78	0.85	0.26	0.14	0.84	0.28	0.84	0.83	0.81	0.60
Totals	**0-5**	**3.89**	**3.61**	**4.09**	**3.09**	**2.76**	**4.07**	**3.18**	**3.60**	**4.00**	**4.57**	**3.62**

References

This annotated reference list reviews the main material from the legal and economic literature on trade secrets. The OECD team has added annotations based on their assessments: key articles are with an asterisk (*) and many of the references have comments in italics on the nature or utility of the item. Appended to the references from the literature is a reference listing of key laws and precedent.

1. Overview: Literature References

This initial scan of the literature found that the economic literature on trade secrets is relatively limited in quantity and scope. It largely falls into three categories: i) fundamental economic theories of trade secret law; ii) theoretical and empirical examination of the trade-offs between patent and trade secret protection; and iii) theoretical and empirical examination of how trade secrecy protection affects firm structure and employee relationships. The legal literature is more expansive in terms of quantity, although much of it is somewhat distant for the purposes of the present project with respect to assessment of economic implications. Also, the United States legal regime for trade secrets is disproportionately represented in the literature.

2. Literature References

AIPPI (1994), *Resolution on Question 115 Effective protection against unfair competition under Article 10bis Paris Convention of 1883*, International Association for the Protection of Intellectual Property (AIPPI), available as of 15 November 2013 at: https://www.aippi.org/download/commitees/115/RS115English.pdf .

Almeling, D.S. et al. (2009), "A Statistical Analysis of Trade Secret Litigation in Federal Courts," *45 Gonzaga Law Review, 291. Descriptive survey of US law.*

Almeling, *D.S. et al. (2010), "*A Statistical Analysis of Trade Secret Litigation in State Courts," *46 Gonzaga Law Review, 57. Descriptive survey of US law.*

AmCham China (2013), "China Business Climate Survey Report: 2013", The American Chamber of Commerce in the People's Republic of China, Beijing.

AMCham Korea (2004), *Intellectual Property Rights*, American Chamber of Commerce in Korea, available as of 13 August 2013 at: http://www.amchamkorea.org/publications/2004ikbc/Intellectual%20Property%20Rights.doc

Ampollini, D. (2010), "Italy" in C. Noorda and S. Hanlose (eds.), *E-Discovery and Data Privacy: A Practical Guide*, Kluwer Law International, Alphen aan den Rijn, The Netherlands.

Anawalt, H.C. (2011), *Idea rights: a guide to intellectual property*, Carolina Academic Press, Durham, N.C.

Anawalt, H.C. and West Group (2011), *IP strategy: complete intellectual property planning, access and protection*, Thomson Reuters/Westlaw, St. Paul, MN.

Andrews, N.H. (1987), "Abuse of Anton Piller Orders," *The Cambridge Law Journal*, 46(1), pp. 50-52.

Aplin, T. and F. Gurry (2012), *Gurry on Breach of Confidence: The Protection of Confidential Information, Section*, Oxford University Press, Oxford, UK.

Arrow, K.J. (1962), "Economic Welfare and the Allocation of Resources for Invention", in *The Rate and Direction of Inventive Activity: Economic and Social Factors*, 609, 615, National Bureau of Economic Research.

Arundel, A. (2001), "The Relative Effectiveness of Patents and Secrecy for Appropriation," 30 *Research Policy*, 611–624.

Arundel, A., G. van de Paal and L. Soete (1995), *"Innovation Strategies of Europe's Largest Industrial Firms: Results of the PACE Survey,"* Directorate General XIII, European Commission, EIMS Publication 23.

ASIS (2007), *Trends in Proprietary Information Loss: Survey Report*, American Society for Industrial Security, ASIS International.

Bai, J.B. and G. Da (2011), "Strategies for Trade Secrets Protection in China," *Northwestern Journal of Technology and Intellectual Property*, 9:351.

Band, T. and I. Miller (2010), *Question Q215: Protection of Trade Secrets Through IPR and Unfair Competition Law, AIPPI Report on Israel.*

Bechtold, S. and F. Hoffler (2011), "An Economic Analysis of Trade-Secret Protection in Buyer-Seller Relationships," *Journal of Law, Economics, and Organization*, 27(1), 137-158.

Bernhardt, D. and V. Dvoracek (2009), "Preservation of Trade Secrets and Multinational Wage Premia," *Economic Inquiry*, 47.4, 726-738.

Biger, N. and S.E. Plaut (2000), "Trade Secrets, Firm-Specific Human Capital, and Optimal Contracting," *European Journal of Law and Economics*, 9.1, 49-71.

Blood, C.G. (2002), "Holding Foreign Nations Civilly Accountable for Their Economic Espionage Practices*," 42 IDEA 227.*

* Bone, R.G. (1998), "A New Look at Trade Secret Law: Doctrine in Search of Justification," *86 California Law Review, 241. Seminal work in the legal literature on trade secret doctrine.*

Bone, R.G. (2011), "Trade Secrecy, Innovation and the Requirement of Reasonable Secrecy Precautions", in R.C. Dreyfuss and K.J. Strandburg (eds.), *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research*, Edward Elgar, Cheltenham, UK.

Brant, J. and S. Lohse (2013), "Enhancing Intellectual Property Management and Appropriation by Innovative SMEs," *Innovation and Intellectual Property Series*, Research Paper No. 1, International Chamber of Commerce.

Budylin, S. and Y. Osipova (2007), "Total Upgrade: Intellectual Property Law Reform in Russia," *Colum. J.E. Eur. L.* 1:1.

Burk, D.L. et al. *(2007),* "The Goldilocks Hypothesis: Balancing Intellectual Property Rights at the Boundary of the Firm," *University of Illinois Law Review, 575.*

Carvalho, N.P.d. (2008), *The TRIPS regime of antitrust and undisclosed information,* Kluwer Law International, Frederick, MD.

Castro, C.R.S. et al. (2012), "Latin Lawyer: Litigation 2013: Brazil", available as of 14 August 2013 at: http://latinlawyer.com/reference/topics/60/jurisdictions/6/brazil/.

Cavazos Cepeda, R., D. Lippoldt and J. Senft (2010), "Policy Complements to the Strengthening of IPRS in Developing Countries", *OECD Trade Policy Papers*, No. 104, OECD Publishing, [TAD/TC/WP(2010)12/FINAL].

CEFIC (2012), *Report on the Importance of Trade Secrets for Chemical Companies*, The European Chemical Industry Council, 15 November.

Cheung, S.N.S. (1982), "Property Rights in Trade Secrets," *Economic Inquiry*, 20, 40-53.

Chiappetta, V. (1999), "Myth, Chameleon or Intellectual Property Olympian - A Normative Framework Supporting Trade Secret Law," *8 George Mason Law Review, 69.*

City Law School (2008), *Employment Law in Practice Section*, Oxford University Press, Oxford, UK.

Claeys, E.R. (2013), "Intellectual Usufructs: Trade Secrets, Hot News, and the Usufructuary Paradigm at Common Law," in S. Balganesh (ed.), *Intellectual Property and the Common Law*, Cambridge University Press, Cambridge, United Kingdom.

Claeys, E.R. (2011), "Private Law Theory and Corrective Justice in Trade Secrecy," 4 *Journal of Tort Law*, Article 2.

Claeys, E.R. (2010), "The Use Requirement at Common Law and Under the Uniform Trade Secrets Act," 33 *Hamline Law Review*, 583. *Explains use requirement and normative justification for it.*

Cohen, W., R. Nelson and J. Walsh (2000), "Protecting their Intellectual Assets: Appropriability Conditions and Why U.S. Manufacturing Firms Patent (Or Not)," *NBER Working Paper*, W7552, http://www.nber.org/papers/w7552.pdf.

Colston, C. and J. Galloway (2010), *Modern Intellectual Property Law*, Routledge, London, UK.

Corrado, C., C. Hulten and D. Sichel (2009), "Intangible Capital and Economic Growth", *Review of Income and Wealth*, Series 55, Number 3, September, pp. 661-685.

Correa, C. (2002), "Unfair Competition under the Trips Agreement: Protection of Data Submitted for the Registration of Pharmaceuticals," 3 *Chi. J. Int'l L.* 69.

Correa, C.M. (2011), "Test data protection: rights conferred under the TRIPS Agreement and some effects of TRIPS-plus standards," in R.C. Dreyfuss and K.J. Strandburg (eds.), *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research*, Edward Elgar, Cheltenham, UK.

Cugno, F. and E. Ottoz (2006), "Trade Secret vs. Broad Patent: The Role Of Licensing," *Review Of Law And Economics*, 2.2, 209-221.

Czapracka, K.A. (2007), "Antitrust and Trade Secrets: The U.S. and the EU Approach," *24 Santa Clara Computer & High Tech Law Journal*, 207.

Di Blasi, G. (2009), "Data Exclusivity Protection in Brazil," World Intellectual Property Review 32, November/December, available as of 13 August 2013 at: http://www.pedrofolio.com/clientes/diblasi/arquivos_pdf/724.pdf.

Dratler, J., Jr. (1990), Trade Secrets in the United States and Japan: A Comparison and Prognosis, *14 Yale J. Int'l L. 68.*

Dreyfuss, R.C. and K.J. Strandburg (2011), "Introduction", in R.C. Dreyfuss and K.J. Strandburg (eds.), *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research*, Edward Elgar, Cheltenham, UK.

* Dreyfuss, R.C. and K.J. Strandburg (eds.) (2011), *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research*, Edward Elgar, Cheltenham, UK. *Collection of papers highlighting a broad range of trade secrets issues ranging from the foundational concepts, to the balance between secrecy and sharing, and the relationship to other public policy areas*.

EC (2013), *Study on Trade Secrets and Confidential Business Information in the Internal Market*, prepared for the European Commission (EC) by Baker and McKenzie, April, available at this link (as of 8 August 2013): http://ec.europa.eu/internal_market/iprenforcement/trade_secrets/index_en.htm#maincontentSec1.

Eisenberg, R.S. (2011), "Data Secrecy in the Age of Regulatory Exclusivity", in R.C. Dreyfuss and K.J. Strandburg (eds.), *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research*, Edward Elgar, Cheltenham, UK.

Ellery, T. and N. Hansen (2012), *Pharmaceutical Lifecycle Management: Making the Most of Each and Every Brand*, Wiley & Sons, Hoboken, N.J., USA.

EOP (2013), *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets*, The Executive Office of the President of the United States (EOP), available as of 29 March 2013 at: http://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf, February.

Fekete, E.K. et al. (2010), *AIPPI Report Q215, Protection of Trade Secrets Through IP and Unfair Competition Law, Brazil*.

Feldman, *Y.* (2003), "Experimental Approach to the Study of Normative Failures: Divulging of Trade Secrets by Silicon Valley Employees*," University of Illinois, Journal of Law, Technology and Policy, 105.*

Fellmeth, A.X. (2004), "Secrecy, Monopoly, and Access to Pharmaceuticals in International Trade Law: Protection of Marketing Approval Data under the TRIPs Agreement," *45 Harvard International Law Journal, 443.*

Fraser Institute (2012), *Economic Freedom of the World 2012 Annual Report*, J. Gwartney, R. Lawson and J. Hall, available as of 15 August 2013 at: http://www.freetheworld.com/reports.html.

* Friedman, D.D., W.M. Landes and R.A. Posner (1991), "Some Economics of Trade Secret Law," *Journal of Economic Perspectives*, 5 (Winter), pp. 61-72. *This seminal paper on the law and economics of trade secrets, sets forth the basic and frequently cited intuitions and models regarding the patent-trade secret trade off and the incentive created by trade secrets.*

Fukao, K., T. Miyagawa, K. Mukai, Y. Shinoda and K. Tonogi (2008), "Intangible Investment in Japan: New Estimates and Contribution to Economic Growth," *RIETI Discussion Paper*, 07-E-034, as revised, June.

Gallié, E-P. and D. Legros (2012), "French firms' strategies for protecting their intellectual property", 41:2 *Research Policy* 780.

Garin, C. (2012), "Customer Poaching Can Now be Punished by Criminal Courts on the Ground of Breach of Trust," Lexology, 24 May, available as of 13 August 2013 at: http://www.lexology.com/library/detail.aspx?g=e11830fd-5222-4084-afdd-a160047f2fec

Ghidini, G. and V. Falce (2011), *Trade secrets as intellectual property rights: a disgraceful upgrading - Notes on an Italian 'reform',* in R.C. Dreyfuss and K.J. Strandburg (eds.), *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research*, Edward Elgar, Cheltenham, UK.

Ghildiyal, S. (2012), Govt working on norms to protect trade secrets, The Times of India, 29 November, available as of 14 August 2013 at: http://timesofindia.indiatimes.com/business/india-business/Govt-working-on-norms-to-protect-trade-secrets/articleshow/17409936.cms.

Gilson, R.J. (1999), "The Legal Infrastructure of High Technology Industrial Districts: Silicon Valley, Route 128, and Covenants Not To Compete," 74 *New York University Law Review, 575.*

Ginarte, J.C. and W. G. Park (1997), "Determinants of Patent Rights: A Cross-National Study," *Research Policy*, Vol. 26, 283-301.

Goodman, C.F. (2004), "Japan's New Civil Procedure Code: Has It Fostered A Rule Of Law Dispute Resolution Mechanism?", *Brook. J. Int'l L.*, 29:511.

Gorodissky Law Firm, (2012), "IP Legislation News," 21 August, available as of 13 August 2013 at: http://www.gorodissky.com/law_news/?newsid=34.

Graham, S. J. H., and T. Sichelman (2008), "Why Do Start-Ups Patent?," *Berkeley Technology Law Journal 23(3), pp. 1063-1097.*

Graham, *S. J. H., R. Merges, P. Samuelson, and T. Sichelman (2010), "High Technology Entrepreneurs and the Patent System: Results of the 2008 Berkeley Patent Survey," Berkeley Technology Law Journal 24(4), pp. 1255-1328.*

Graves, C.T. (2011a), "Analyzing The Non-Competition Covenant as a Category of Intellectual Property Regulation," *3 Hastings Science and Technology Law Journal*, 69.

Graves, C.T. (2011b), "Trade secrecy and common law confidentiality: the problem of multiple regimes", in R.C. Dreyfuss and K.J. Strandburg (eds.), *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research*, Edward Elgar, Cheltenham, UK.

Graves, C.T. and J.A. DiBoise (2007), *"*Do Strict Trade Secret and Non-Competition Laws Obstruct Innovation?," *1 Ohio State Entrepreneurial Business Law Journal, 231.*

Grishchenkova, A. (June 2012), "The Discovery Process in Russia. Will the New Era Come?," FBK Legal, available as of 14 August 2013 at: http://www.legal500.com/developments/20074.

Grubbs, S.R. (ed.) (2003), International Civil Procedure, Kluwer Law International, The Hague, Netherlands.

Hailing, S (2010), *Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, China*.

Hall, B. H., C. Helmers, M. L. Rogers and V. Sena (2012), "The Choice Between Formal and Informal Intellectual Property: A Literature Review," NBER Working Paper No. w17983. Available at SSRN: http://ssrn.com/abstract=2035782 (as of 31 October 2012).

* Hogan Lovells (2012), *Study on Trade Secrets and Parasitic Copying (Look-alikes)*, MARKT/2010/20/D, Report on Trade Secrets for the European Commission, Hogan Lovells

International LLP. *This review of protection of trade secrets in the European Union is an excellent source of baseline information.*

Instituto Mexicano de la Propriedad Industrial (2013), "Protección De Los Secretos Industriales En México, Conforme A Los Parámetros Del Documento."

Ivanov, Y., "Non-Compete Clause in Russia: Do the Laws Compete?," The Moscow Times, 16 October 2008, available as of 14 August 2013 at: http://www.themoscowtimes.com/business_for_business/article/non-compete-clause-in-russia-do-the-laws-compete/371717.html#ixzz2RnClzTM9 .

Jager, M.F. (2012), *Trade Secrets Law*, Thompson-Reuters, Westlaw. *This is a comprehensive legal treatise.*

Johnson, E.E. (2010), "Trade Secret Subject Matter," 33 *Hamline Law Review*, 545.

Jones, J (2007), "Data exclusivity provisions under the Therapeutic Goods Act 1989," available as of 14 August 2013 at: http://www.davies.com.au/pub/detail/234/data-exclusivity-provisions-under-the-therapeutic-goods-act-1989.

Khabarov, D.I. (2012), "Intellectual Property – Russia," International Law Office, January.

Kim, H.S. (2011), "Trade secret law, intellectual property, and innovation: Theoretical, empirical, and Asian perspectives," PhD Thesis, University of Illinois.

Kim, S.R. (2010), *Protection of Trade Secrets Through IP and Unfair Competition Law*, AIPPI Report Q215, Korea.

* *Kitch*, E.W. (1980), "The Law and Economics of Rights in Valuable Information," *9 Journal of Legal Studies, 683. Another seminal article.*

Knobel, J. (2000), "Wrongfulness Of Trade Secret Misappropriation; and Trade Secrets As Objects Of Subjective Rights," *Acta Juridica* 2000:196.

Koch, M. (2006), *Non-competition clauses in labour contracts, Sweden, Report for the XIVth Meeting of European Labour Court Judges*, available as of 14 August 2013 at: http://www.ilo.org/wcmsp5/groups/public/@ed_dialogue/@dialogue/documents/meetingdocument/wcms_159972.pdf.

Lai, E. L-C., R. Riezman and P. Wang (2009), "Symposium on Organization, Heterogeneity and Trade: Outsourcing of Innovation," *Economic Theory*, 38.3, 485-515.

Landes, W.M. and R.A. Posner (2003), "The Economics of Trade Secrecy Law," in the *Economic Structure of Intellectual Property Law*, Harvard University Press, Cambridge, MA. *A follow up to and summary of a 1991 article.*

* Landes, W.M. and R.A. Posner (2003), *The Economic Structure of Intellectual Property Law*, Harvard University Press, Cambridge, MA.

Lang, J. (2003), "The Protection of Commercial Trade Secrets," *European Intellectual Property Review*, 10:462.

Lee, H.P. and E. Campbell (2013), *The Australian Judiciary*, Cambridge University Press, Cambridge, UK.

Leiponen, A. and J. Byma (2009), "If You Cannot Block, You Better Run: Small Firms, Cooperative Innovation, And Appropriation Strategies," *Research Policy*, 38.9, 1478-1488.

* Lemley, M.A. (2008), "The Surprising Virtues of Treating Trade Secrets as IP Rights", *61 Stanford Law Review, 311. This paper contends that trade secret law leads to greater spillovers and more information sharing because the presence of the law leads owners to forego more restrictive forms of physical or other security.*

Lemley, M.A. (2011), "The Surprising Virtues of Treating Trade Secrets as IP rights", in R.C. Dreyfuss and K.J. Strandburg (eds.), *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research*, Edward Elgar, Cheltenham, UK.

* Lerner, J. (1994), "The Importance of Trade Secrecy: Evidence from Civil Litigation," unpublished manuscript, Harvard University, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=6089. *Establishes importance of trade secrets to SMEs in the United States.*

Lester, G. (2001), "Restrictive Covenants, Employee Training, and the Limits of Transaction-Cost Analysis," *76 Indiana Law Journal, 49.*

Levin, M. et al. (2010), *Protection of Trade Secrets Through IP and Unfair Competition Law,* AIPPI Report Q215, Sweden.

Levine, D. (2010), "What Can the Uniform Trade Secrets Act Learn From the Bayh Dole Act," *33 Hamline Law Review, 615.*

Liang, D. (April 2008), "The Interplay of Non-compete Covenants under the PRC Anti-monopoly Law," King Wood & Mallesons China Bulletin, available as of 14 August 2013 at: http://www.kingandwood.com/article.aspx?id=The-Interplay-of-Non-compete-Covenants-under-the-PRC-Anti-monopoly-Law-04-china-bulletin-2008&language=en.

Lippoldt, D.C. (2011), *Patent Rights, Developing Countries and the Economic Influence of the Multilateral Trading System*, SciencesPo, Paris, http://spire.sciences-po.fr/hdl:/2441/f4rshpf3v1umfa09lass9h1s2.

Liuzzo, L. et al. (2010), *Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, Italy*.

MacLaren, T. (2012), *Trade Secrets Throughout the World*, database update, Thomson/West, Eagan, MN, USA.

Maleshin, D. (2007), "The Russian Style of Civil Procedure," *Emory Int'l L. Rev*. 21:543.

Malsberger, B.M., R.A. Blackstone and A.H. Pedowitz (2006), *Trade Secrets: A State-by-State Survey*, Bureau of National Affairs, Washington D.C.

Maskus, K. E. (2000), *Intellectual Property Rights in the Global Economy*, Institute for International Economics.

Maskus, K.E. (2012), *Private Rights and Public Problems: The Global Economics of Intellectual Property in the 21st Century*, Peterson Institute for International Economics.

McAfee (2009), *Unsecured Economies: Protecting Vital Information.*

McAfee (2011), *Underground Economies: Intellectual Capital And Sensitive Corporate Data Now The Latest Cybercrime Currency*.

MacLaren, T. (2013), *Eckstrom's Licensing in Foreign and Domestic Operations: Joint Ventures*, database update, Thomson/West, St. Paul, MN, USA.

McGuire, M. et al., *Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215*.

* Merges, R.P. (1999), "The Law and Economics of Employee Inventions", *13 Harvard Journal of Law and Technology, 1. An important theoretical work on the interaction of trade secret law with ownership of employee inventions.*

Milgrim, R.M. and E.E. Bensen (1997), *Milgrim on trade secrets,* M. Bender, New York, NY. *Comprehensive legal treatise.*

Moohr, G.S. (2002), "The Problematic Role of Criminal Law in Regulating Use of Information: The Case of the Espionage Act," *80 North Carolina Law Review, 853.*

Nemec, D. and K. Voorhees (2013), "Recent amendment to the Economic Espionage Act extends protection against misappropriation, Thomson Reuters News & Insight, 13 February.

OECD (2010), *Measuring Innovation: A New Perspective*.

OECD (2011), *New sources of growth: intangible assets*, a flyer available on-line: http://www.oecd.org/sti/inno/46349020.pdf.

Office of the National Counterintelligence Executive Report (2011), *Foreign Spies Stealing US Economic Secrets in Cyberspace*.

Osakwe, C. (2008), *Russian Civil Code. Parts 1 -3: Text and Analysis*, Wolters Kluwer, Moscow, Russia.

Paalanen-Koev, H. (2012), *Corporate Counsel's Guide to Doing Business in Russia*, Thomson/West, St. Paul, MN, USA.

Park, W.G. (2008), "International Patent Protection: 1960-2005", *Research Policy*, No. 37, 761-766.

Park, W.G. and D.C. Lippoldt (2003), "The Impact of Trade-Related Intellectual Property Rights on Trade and Foreign Direct Investment in Developing Countries", *OECD Papers*, Vol. 3, No. 11, paper 294, [TD/TC/WP(2003)10/FINAL].

Park, W.G. and D.C. Lippoldt (2005), "International Licensing and the Strengthening of Intellectual Property Rights in Developing Countries", *OECD Trade Policy Working Paper* #10, Paris, [TD/TC/WP(2004)31/FINAL]. (This paper was further developed and released in OECD Economic Studies, 2005, Vol. 40.)

Park, W.G. and D.C. Lippoldt (2008), Technology Transfer and the Economic Implications of the Strengthening of Intellectual Property Rights in Developing Countries, *OECD Trade Policy Paper*, Number 62, OECD, January, [TAD/TC/WP(2007)19/FINAL].

PhRMA (2013), *Special 301 Submission 2013*, available as of 14 August 2013 at: http://www.phrma.org/sites/default/files/pdf/PhRMA%20Special%20301%20Submission%202013.pdf

Png, I. (2012a), *Law and Innovation: Evidence from State Trade Secrets Laws*, mimeo, National University of Singapore, SSRN.

* Png, I. (2012b), "*Trade Secrets, Non-Competes, and Mobility of Engineers and Scientists: Empirical Evidence",* mimeo, National University of Singapore, SSRN. *Creates and uses a small index of trade secret strength.*

Pooley, J. (1997), *Trade Secrets*, Law Journal Seminars-Press, New York, NY. *Comprehensive legal treatise, with annual supplements*.

Practical Law Company (April 2013), "IP in business transactions: South Africa overview", available as of 14 August 2013 at: http://uk.practicallaw.com/6-519-5891#a480193.

Quinto, D.W. and S.H. Singer (2009), *Trade secrets: law and practice*, Oxford University Press, NY.

Rajbhandary, A. (1996), "Protecting Trade Secrets Through Family Businesses: A Case Study On Nepal," *International Review of Law and Economics*, 16.4, 483-490.

Rapsinews (2011), "Court allows BP not to disclose information on Rosneft deal," 10 October, available as of 14 August 2013 at: http://www.rapsinews.com/judicial_news/20111010/256186687.html.

Rapsinews (2011), "Coal producer secures hearing for suit against antimonopoly service," 30 September, available as of 14 August 2013 at: http://www.rapsinews.com/judicial_news/20110930/255926069.html/

Reagan, T. and J. Cort (2009), *Sealed Cases in Federal Courts*, Federal Judicial Center, available as of 14 August 2013 at: http://www.fjc.gov/public/pdf.nsf/lookup/sealcafc.pdf/$file/sealcafc.pdf

Reddy, P. (2013), "The Data Exclusivity Debate in India: Time for a rethink?," available as of 14 August 2013 at: http://ssrn.com/abstract=2231027 .

Reuters, "German Spy Chief Targets Russian, Chinese Industrial Espionage," 18 February 2013, at: http://www.reuters.com/article/2013/02/18/us-germany-spies-idUSBRE91H08C20130218

Revue Lamy Droit de L'immatériel (2007) No. 27, 05-2007.

Risch, M. (forthcoming, 2012), "An Empirical Look at Trade Secret Law's Shift from Common to Statutory Law," in S. Balganesh (ed.), *Intellectual Property and the Common Law*. Cambridge University Press, Cambridge, UK.

* Risch, M. (2011), "Trade secret law and information development incentives", *in* R.C. Dreyfuss and K.J. Strandburg (eds.), *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research*, Edward Elgar, Cheltenham, UK.

Risch, M. (2010), "A Failure of Uniform Laws?*"*, 159 *University of Pennsylvania Law Review*, 1

Risch, M. (2009), "Comments on Trade Secrets Sharing in High Velocity Labor Markets," 12 *Employment Rights and Employment Policy Journal*, 339.

* Risch, M. (2007), *"Why Do We Have Trade Secrets,"* 11 *Marquette Intellectual Property Law Review*, 1. *This author contends that the most important marginal incentive created by trade secrets is to reduce wasteful spending on security or circumventing security. He argues that trade secret law provides a less important marginal incentive to invest in R&D because it requires secrecy, and where parties can keep an innovation secret, they already have an incentive to innovate without trade secret law.*

Ronde, T. (2001), "Trade Secrets and Information Sharing", *Journal of Economics & Management Strategy*, 10, 391-417.

Rowe, E and S.K. Sandeen (forthcoming 2012), *Rowe and Sandeen's Cases and Materials on Trade Secret Law*, Thomson Reuters/Westlaw, St. Paul, MN.

* Samuelson, P. and S. Scotchmer (2002), "The Law and Economics of Reverse Engineering," *111 Yale Law Journal, 1575. A well-cited article on the theory supporting the allowance of reverse engineering.*

Sandeen, S.K. (2011), "The limits of trade secret law: Article 39 of the TRIPS Agreement and the Uniform Trade Secrets Act on which it is based," *in* R.C. Dreyfuss and K.J. Strandburg (eds.), *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research*, Edward Elgar, Cheltenham, UK.

Sanger, D. and N. Perlroth (2013), "Chinese Hackers Resume Attacks on U.S. Targets," New York Times, A1, 19 May, available as of 13 August 2013 at: http://www.nytimes.com/2013/05/20/world/asia/chinese-hackers-resume-attacks-on-us-targets.html?_r=0 .

Schacht, W.H. and J.R. Thomas (2011), *Follow-On Biologics: The Law and Intellectual Property Issues*, Congressional Research Service, Washington, D.C.

Seyoum, B. (1993), "Property Rights Versus Public Welfare in the Protection of Trade Secrets In Developing Countries," *International Trade Journal*, 7.3, 341-360. *More argumentative than theoretical and empirical, it nevertheless contains some arguments regarding trade secrets' impact on developing countries.*

Sherby, E. (2004), *A Primer on Commercial Litigation in Israel*, available as of 13 August 2013 at: http://www.sherby.co.il/Primer.pdf.

* Sherwood, R.M. (1990), *Intellectual Property and Economic Development*, Westview Special Studies in Science, Technology, and Public Policy. *Excellent case studies regarding IP laws, including trade secrets, in developing countries.*

* Sichelman, T. and S.J.H. Graham (2010), "Patenting by Entrepreneurs: An Empirical Study," *17 Michigan Telecommunications & Technology Law Review*, 111, *Analysis of entrepreneurs' choices of patents vs. trade secrets.*

Singh, H. (2010), *"Protection of Trade Secrets through IP and Unfair Competition Law," AIPPI Report Q215*.

Sirota, A (2011), "On contributing know-how in capital of Russian company," available as of 14 August 2013 at: http://www.russianlawonline.com/content/contributing-know-how-capital-russian-company.

Stankovic, M. (2010), "Trade Secrets: South Korea versus United States," reference available as of 14 August 2013 at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1678768 .

Stouls, J.P. et al. (2010), *Protection of Trade Secrets Through IP and Unfair Competition Law*, AIPPI Report Q215, France.

Sumpter, P. (2006), *Intellectual Property Law: Principles in Practice*, CCH New Zealand, Auckland.

Toutoungi, A. (16 August 2012), "Trade Secrets Move (Slowly) Up the Agenda," Eversheds International Website, http://www.eversheds.com/global/en/what/articles/index.page?ArticleID=en/Industrial_engineering/Trade_secrets_move-slowly-up_the_agenda.

US Department of State (March 2011), *2011 Investment Climate Statement – Republic of Korea*, http://www.state.gov/e/eb/rls/othr/ics/2011/157359.htm.

Ubukata, K. (2010), *Question Q215: Protection of Trade Secrets Through IPR and Unfair Competition Law*, AIPPI Report on Japan.

UK Law Commission (1981), *Report on Breach of Confidence*, Law Com No.110.

UK Law Commission (1997), *Misuse of Trade Secrets Consultation Paper*, available as of 14 August 2013 at: http://lawcommission.justice.gov.uk/docs/cp150_Legislating_the_Criminal_Code__Misuse_of_Trade_Secrets_Consultation.pdf.

US National Science Foundation (2012), "Business Use of Intellectual Property Protection Documented in NSF Survey," *NSF Infobrief* 12-307, National Center for Science and Engineering Statistics.

USTR (2012), *2012 Special 301 Report*, Office of the United States Trade Representative.

USTR (2007), *2007 Special 301 Report*, Office of the U.S. Trade Representative.

Vaidyanathan, R.K. (2010), "Trade Secrets and Confidential Information," Advaya Legal Law Firm Website, September.

Vos, A. (2008), "South Africa: Discovery of Confidential Documents," Mondaq.com, 13 November, available as of 14 August 2013 at: http://www.mondaq.com/x/69448/Discovery+Of+Confidential+Documents.

WTO (2012), Trade Policy Review Body – Report by the Secretariat – Israel, WT/TPR/S/272, 52 (25 September 2012), World Trade Organization.

Zabojnik, J. (2002), "A Theory of Trade Secrets in Firms," *International Economic Review*, 43, 831-55.

3. Selected Laws and Precedent

This section lists the most significant statues governing trade secrets in the jurisdictions conveyed. In the case of common law jurisdictions with few or no statutes governing trade secrets, this listing contains citations to significant cases.

Australia

Statutes

- Australia Therapeutic Goods Act 1989
- Agricultural and Veterinary Chemicals Code Act 1994

Cases

- Coco v. A.N. Clark (Engineers) Ltd. [1969] RPC 41 (English law)
- Franklin v. Giddins [1978] Qd R 72
- Mainbridge Industries Pty. Ltd. v. Whitewood (1984) 73 FLR 117.
- Moorgate Tobacco Co. Ltd. v. Philip Morris Ltd. (No. 2) (1984) 156 CLR 414
- Searle Australia Pty. Ltd. v. Public Interest Advocacy Center & Anor (1992) 36 FCR 111

Brazil

Statutes

- Article 195, Sections XI – XII Law No. 9.279 of May 14, 1996 (Industrial Property Law).

China

Statutes

- Article 10, Unfair Competition Law of the People's Republic of China (promulgated by the Standing Comm. Nat'l People's Cong., Sept. 2, 1993, effective Sept. 2, 1993
- Article 22 of the Labor Law
- Article 43 of the Contract Law

France

Statutes

- Article L. 621-1 of the Intellectual Property Code
- Article L. 1227-1 of the Labor Code
- Article 1392 of the Civil Code
- Article 226-13 of the Criminal Code
- Article 311-1 of the Criminal Code
- Article 314-1 of the Criminal Code

Germany

Statutes

- Act Against Unfair Competition of 1909 (UWG)

India

Statutes

- 46th Report on the "Pesticide Management Bill, 2008," Department Related Parliamentary Standing Committee on Agriculture (2008)

Cases

- AIA Engineering Pvt. Ltd. v. Bharat Dand and Ors., AIR 2007 Gujarat (NOC) 1456
- Bank Ltd. v. Priya Puri, (2006) IIILLJ 540 Del.; Bombay Dyeing and Manufacturing Co. Ltd. v. Mehar Karan Singh, 2010 (112) BomLR3759
- Escorts Construction v. Action Construction, 1999 PTC 36 (Del)
- Konrad Wiedemann GmbH v. Standard Castings Pvt. Ltd., [1985](10) IPLR 243; Mr. Diljeet Saltman Engineering Co. v. Campbell Engineering Co. Ltd., [1948] 65 RPC 203 (English law)
- Titus, Advocate v. Mr. Alfred A. Adebare and Ors., 2006 (32) PTC 609 (Del); American Express

Israel

Statutes

- Commercial Torts Law, Section 5, Israel - Unfair Competition (Commercial Torts). World Intellectual Property Organization, Law, 19/04/1999 -5759(il012), Available at: http://www.wipo.int/clea/docs_new/pdf/en/il/il012en.pdf

Italy

Statutes

- Legislative Decree No. 30 of 10 February 2005 and amended by Legislative Decree No. 131 of 13 August 2010, under the header "Secret information".
- Article 99 IPC, as amended by Legislative Decree No. 131 of 13 August 2010.
- Articles 621, 622 and 623 of the Italian Criminal Code.
- Article 2598 of the Italian Civil Code.

Japan

Statutes

- Article 1(6), Unfair Competition Prevention Act (Act No. 47 of 1993) (up to the revisions of Act No. 62 of 2011 (Effective December 1, 2011)), unofficial translation available at http://www.wipo.int/wipolex/en/text.jsp?file_id=254517.

New Zealand

Statutes

- Section 230(2) of the Crimes Act 1961

Cases

- AB Consol. Ltd. v. Europe Strength Food Co. Pty. Ltd., [1978] 2 NZLR 515
- Aquaculture Corp. v. New Zealand Green Mussel Co. Ltd. (No. 1), (1985) 5 IPR 353
- Coco v. A.N. Clark (Engineers) Ltd. [1969] RPC 41 (English law)
- Fisher & Paykel Finance v Karum, [2012] NZHC 331
- SSC&B: Lintas New Zealand Ltd. v. Murphy & Anor, (1986) 3 NZCLC 99,546

Republic of Korea

Statutes

- Trade Secrets Act, Article 1, Para. 2.

Russia

Statutes

- Civil Code Article 1465 (2011)
- Civil Code Article 1466(2) (2011)
- Civil Code Article 1467 (2011)

- Civil Code Article 1472(2)(2) (2011)
- Article 183(1), Criminal Code of the Russian Federation No. 63-FZ of June 13, 1996 (as last amended on June 29, 2009)
- Federal Law Commercial Secrecy, No. 98-FZ, Article 10 (July 29, 2004) (as amended July 24, 2007)

South Africa

Cases

- Advtech Resourcing (Pty) Ltd v Kuhn 2007(4) ALL SA 1386 ,C para51
- Bambelela Bolts (Pty) Ltd v Ball and Another (J 2977/11) [2012] ZALCJHB 148
- Document Warehouse (Pty) Limited v Truebody and Another (2010/26977) [2010] ZAGPJHC 92 (13 October 2010)
- Dun and Bradstreet (Pty) Ltd v SA Merchants Combined Credit Bureau (Cape) (Pty) Ltd., (1968) 1 SA 209

Sweden

Statutes

- Act on the Protection of Trade Secrets (SFS 1990:409).

United Kingdom

Cases

- Attorney General v. Guardian Newspapers Ltd. (No. 2), [1988] 3 All ER 545.
- Coco v. A.N. Clark Eng'rs Ltd., [1969] RPC 41
- Exchange Telegraph Co. Ltd. v. Central News Ltd., [1897] 2 Ch. 48Lansing Linde Ltd v Kerr, [1991] 1 W.L.R. 251
- Faccenda Chicken Ltd. v. Fowler, [1986] 1 All ER 617
- House of Lords in Herbert Morris, Ltd. v. Saxelby, [1916] 1 AC 688
- Mustad v. Allcock and Dosen, [1963] 3 All ER 416
- Saltman Engineering Co. v. Campbell Engineering Co. Ltd. [1948] 65 RPC 203

United States

Statutes

- Espionage Act of 1996, as amended: 18 USC § 1831 and § 1832
- EPA Pesticide Registration Manual, Chapter 10 (2010), http://www.epa.gov/pesticides/bluebook/chapter10.html
- First Restatement of Torts § 737 (1939)
- Uniform Trade Secrets Act Section 1, available at: http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf

Annex 1: Country Charts and Preliminary Index Scoring

Overview

This annex provides a detailed snapshot of trade secrets protection, focusing on those elements that were considered in the development of the preliminary Trade Secrets Protection Index. For each of the 21 countries in the sample, the annex presents: (1) a chart with descriptive text for each element and (2) a table with the detailed scoring for those elements retained in the preliminary index.

A standard template was utilized for the **Annex Chart**. The elements concerning the legal framework for trade secret protection were formulated in a manner conducive to giving a status report in an objective and verifiable fashion. In addition, the chart includes two further items concerning the operation of the system in practise: (1) a legal complements rating and (2) expert characterization.

The legal complements rating provides an indication of the functioning of the legal system in practise. It presents a score based on a component of the Fraser Institute's *Index of Economic Freedom*. The component is entitled "*Legal System and Security of Property Rights*." This component takes into account judicial independence, impartiality of courts, protection of property rights, military interference in the rule of law and politics, integrity of the legal system, legal enforcement of contracts, regulatory restrictions on the sale of real property, reliability of the police and business costs of crime.[1]

The expert characterization element for each country is presented at the end of each country's chart. The entries provide qualitative information on the operation of the legal system with respect to the available protection for trade secrets. They are based on expert commentary from recognized, published sources by governments, professional associations, attorneys, and legal scholars.

The **Annex Table** provides the detailed scoring of the preliminary Trade Secrets Protection Index for each country. The index consists of five components, each with a maximum score of 1; the maximum score for the index is 5. The score for each component is the sum of the scores obtained for the relevant elements divided by the total number of individual elements for the component. In other words, each component score is normalized to fall on a scale of zero to one.

[1] In developing its index, the Fraser Institute describes its approach as follows, "First, objective components are always preferred to those that involve surveys or value judgments. Given the multidimensional nature of economic freedom and the importance of legal and regulatory elements, it is sometimes necessary to use data based on surveys, expert panels, and generic case studies. To the fullest extent possible, however, the index uses objective components. Second, the data used to construct the index ratings are from external sources such as the International Monetary Fund, World Bank, and World Economic Forum that provide data for a large number of countries. Data provided directly from a source within a country are rarely used, and only when the data are unavailable from international sources. Importantly, the value judgments of the authors or others in the Economic Freedom Network are never used to alter the raw data or the rating of any country. Third, transparency is present throughout." See pp. 3 and 273-5, Gwartney, J., R. Lawson and J. Hall (2012), *Economic Freedom of the World: 2012 Annual Report*, The Fraser Institute, available on-line at: http://www.freetheworld.com/ .

Annex Chart

AUSTRALIA

Source of Law, Definition and Scope

Statutory or Other Protection		**Definition**			**Additional Elements of Definition**					**Scope**	
Civil	Criminal	All confidential business information	Common Definition: Confidential business information, **subject to:** deriving value from secrecy; making reasonable efforts to maintain secrecy	Common definition **plus condition that** it be imparted to recipient in confidence	Use must be shown	Inventory of trade secrets required	Must be reduced to writing	Must be identified as a trade secret to recipient	Written notice to recipient required	Confidential Business Information	Technical Information
Comprehensive civil protection by means of common law.	None.	No.	Yes.	Yes, but confidential relationship created via constructive trust, at least where defendant engaged in tortious or criminal act.	No.	No.	No.	No.	No.	Yes.	Yes.

AUSTRALIA

Covered Acts

Acts Covered as Civil Infringement		**Acts Covered as Crimes**		**Third Parties:** **Liable for Acquisition?** **Liable Even if Innocent (Without Knowledge)?**	
Breach of Duty?	Wrongful Acquisition / Misappropriation	Breach of Duty?	Wrongful Acquisition / Misappropriation	Civil	Criminal
Use in Breach of Duty. Disclosure in Breach of Duty.	Yes, via imposition of a constructive trust, at least where defendant engaged in tortious or criminal act.	Not applicable.	Not applicable.	Yes. Innocent recipients can be enjoined.	Not applicable.

AUSTRALIA

Defining Duties and Misappropriation

Defining Duty of Confidentiality			**Restrictions on Duty of confidentiality**		**Defining Wrongful Acquisition - Misappropriation**	
Commercial Relationship	Current Employment Relationship	Past Employment Relationship	Commercial Relationship	Employment Relationship	Civil	Criminal
Duty can be based on express agreement in commercial contract. Duty can be implied in the context of a business relationship.	Duty can be based on express agreement and implied duty. Implied duty broad during employment – covers information beyond strict trade secret definition.	Duty can be based on express contract. Duty is also implied. Implied duty narrower after employment – only trade secrets. No inevitable disclosure doctrine.	None.	Express agreements may cover general skills and knowledge. Implied post-employment duties to keep information confidential unenforceable with respect to general skills and knowledge.	Yes, via imposition of a constructive trust, at least where defendant engaged in tortious or criminal act.	Not applicable.

AUSTRALIA

Restrictions on Liability

Additional Elements of Proof in Infringement Claim		**Contractual Restrictions on Competition - Validity**		**Defences**	
Civil	Criminal	Commercial Relationship	Post-Employment	Civil	Criminal
Detriment must be shown.	Not applicable.	Commercial agreements not to compete generally enforceable.	Post-employment agreements not to compete enforceable if reasonable with respect to time and geographic scope.	Independent creation. Reverse engineering.	Not applicable.

AUSTRALIA

Remedies

Civil Remedies								**Criminal Remedies**
Injunction to eliminate wrongful head start	Delivery up and/or destruction of infringing materials	Compensatory Damages – Availability and Type	Defendant's Profits	Punitive damages available?	Statutory or Pre-established damages	Fines	Jail Sentence	Other
Yes, even where information has since become public.	Yes.	Out of pocket. Lost Profits. Consequential.	Yes.	No.	No.	Not applicable.	Not applicable.	Not applicable.

AUSTRALIA

Enforcement, investigation and discovery & related regulations

Enforcement, investigation and discovery			**Data Exclusivity**		**Technology Transfer**	**Legal Complements**
Emergency Search to preserve and obtain proof	Pre-trial discovery	Protection of confidentiality of trade secrets in litigation	Drugs	Agricultural Chemicals		Fraser Score
Ex parte available. Plaintiff may conduct search.	Documentary. At initiative of party.	Full protection with respect to hearings (in camera hearings available). No protection from other party (protective orders, measures limiting viewing to counsel or other professionals).	New chemical entities only. Drugs: 5 years. Agricultural and veterinary: 11 years.	With respect to agricultural and veterinary products, the exclusivity period is 5 years if the same data is used to register another *agricultural* product or to change labelling, or 3 years if the same data is used to register another *veterinary* product or to change labelling.	None.	On the Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, Australia receives a score of 8.1 out of 10, which ranks it 13th in the world.

AUSTRALIA

Additional Comments

Expert characterisation of the operation of the protection of trade secrets in practice
Criticism of Australian trade secret law is minimal. An AIPPI group encouraged greater protection in litigation: "The Australian Group considers that promotion of effective protection of confidential information lies in providing greater certainty regarding the treatment of confidential information in litigation." Rodney De Boos, et al., Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, Australia 9 (2010).

SOURCES:

See Annex 2 of this paper for a detailed overview of Australian trade secret law and sources.

BRAZIL

Source of Law, Definition and Scope

Statutory or Other Protection		**Definition**			**Additional Elements of Definition**					**Scope**	
Civil	Criminal	All confidential business information	Common Definition: Confidential business information, **subject to:** deriving value from secrecy; reasonable and making reasonable efforts to maintain secrecy	Common definition **plus condition that** it be imparted to recipient in confidence	Use must be shown	Inventory of trade secrets required	Must be reduced to writing	Must be identified as a trade secret to recipient	Written notice to recipient required	Confidential Business Information	Technical Information
Comprehensive civil protection pursuant to statute.	Comprehensive criminal protection pursuant to statute.	No.	Yes.	No.	No.	No.	No.	No.	No.	Yes.	Yes.

BRAZIL

Covered Acts

Acts Covered as Civil Infringement		**Acts Covered as Crimes**		**Third Parties:** **Liable for Acquisition?** **Liable Even if Innocent (Without Knowledge)?**	
Breach of Duty?	Wrongful Acquisition / Misappropriation	Breach of Duty?	Wrongful Acquisition / Misappropriation	Civil	Criminal
Only for (a) employees; (b) fiduciaries such as business partners; and (c) others who have signed non-disclosure agreements. Trade secret licenses in technology transfer agreements are generally disapproved, rendering breach of duty unavailable in many common commercial arrangements such as franchising, outsourcing, joint ventures, and the like.	Yes.	Only for (a) employees; (b) fiduciaries such as business partners; and (c) others who have signed non-disclosure agreements. Trade secret licenses in technology transfer agreements are generally disapproved, rendering breach of duty unavailable in many common commercial arrangements such as franchising, outsourcing, joint ventures, and the like.	Yes.	Yes. No. Only liable if third party has knowledge or reason to know.	Yes. No. Only liable if third party has knowledge or reason to know.

BRAZIL

Defining Duties and Misappropriation

Defining Duty of Confidentiality			**Restrictions on Duty of confidentiality**		**Defining Wrongful Acquisition - Misappropriation**	
Commercial Relationship	Current Employment Relationship	Past Employment Relationship	Commercial Relationship	Employment Relationship	Civil	Criminal
Duty can be based on express contract or implied. Duty not to disclose, exploit, or use.	Duty can be based on express contract or implied. Implied duty will be basis for termination of employment Duty not to disclose, exploit, or use.	Duty can be based on express agreement or implied. No doctrine of inevitable disclosure.	The technology transfer requirements discussed below severely restrict the duty of confidentiality in many common commercial agreements, specifically those involving trade secret licenses. Ends with public disclosure of confidential information.	Ends with public disclosure of confidential information.	Obtaining secrets by fraud, espionage, or other illegal means.	Obtaining secrets by fraud, espionage, or other illegal means.

BRAZIL

Restrictions on Liability

Additional Elements of Proof in Infringement Claim		**Contractual Restrictions on Competition - Validity**		**Defences**	
Civil	Criminal	Commercial Relationship	Post-Employment	Civil	Criminal
None.	None.	May be struck from agreement by administrative authorities or courts if viewed as a violation of competition law.	Must be related to the protection of trade secrets, limited in duration and geographic scope. Must provide remuneration to employee. No doctrine of inevitable disclosure.	Independent creation. Reverse engineering.	Independent creation. Reverse engineering.

BRAZIL

Remedies

Civil Remedies								**Criminal Remedies**		
Preliminary injunction	Permanent injunction	Injunction to eliminate wrongful head start	Delivery up and/or destruction of infringing materials	Compensatory Damages – Availability and Type	Defendant's Profits	Punitive damages available?	Statutory or Pre-established damages	Fines	Jail Sentence	Other
Yes. Temporary restraining orders and other ex parte action available.	Yes (For so long as remains secret).	Uncertain.	Yes.	Material -Compensatory. -Consequential. -Royalties. Moral. Parties often specify fines in contracts, which are an enforceable remedy.	Yes.	Yes, in theory, but no case law on this point.	No.	Unspecified but expert opinion indicates they are not substantial.	Three months to one year.	

BRAZIL

Enforcement, investigation and discovery & related regulations

Enforcement, investigation and discovery			Data Exclusivity		Technology Transfer	Legal Complements
Emergency Search to preserve and obtain proof	Pre-trial discovery	Protection of confidentiality of trade secrets in litigation	Drugs	Agricultural Chemicals		Fraser Score
Yes. Ex parte available.	Limited to production of documents under supervision of court.	In camera hearings available. Protection of documents available. No protection from other party other than order not to reveal.	None currently. The Brazilian Pharmaceutical Regulatory Agency may approve a generic drug application based on prior approval of a new chemical entity at any time.	10 years for agricultural products and veterinary drugs if new chemical entity. 5 years for new uses and indications.	Registration and approval of IP license agreements required. Essential terms of trade secret licenses are regulated. First, there is doubt that a trade secret can be licensed, rather than transferred. Second, the following provisions are **prohibited:** (1) limiting use of information after expiration of agreement; (2) requiring return of materials (e.g., documents) at the termination of the agreement; and (3) providing an unlimited term (terms are typically limited to 19 years at the most).	On the Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, Brazil receives a score of 5.24 out of 10, which ranks it 77th in the world.[33] Its lowest scores are with respect to integrity of the legal system (3.33 out of 10) and reliability of police (3.97 out of 10).[34]

33 Fraser Institute, Economic Freedom of the World 2012 Annual Report at 46 (2012).

34 Ibid.

BRAZIL

Additional Comments

Expert characterisation of the operation of the protection of trade secrets in practice
"Because few cases have been tested in court, Brazil lacks a substantial jurisprudence on trade secrets."[35] Note that in Brazil, a private party may initiate a criminal trade secret suit and may also pursue civil remedies. Thus, the process for seeking a remedy for trade secret infringement may encompass a criminal and civil proceeding, with all remedies from both kinds of actions available. However, criminal penalties are relatively low: Violation of trade secrets (and of Industrial Property rights in general) is treated by our statutory law as a "crime of lower offensive potential". Penalties foreseen are low ("detention of 3 (three) months to 1 (one) year) or a fine") and their lack of effectiveness together with the difficulties to recover damages create relative values and enforcement difficulties. Major challenges for effectively enforcing trade secrets in Brazil and entering agreements with other businesses concerning trade secrets are the Brazilian Patent and Trademark Office's ("BPTO") role in approving license agreements for intellectual property. The BPTO disapproves of trade secret licenses, and there are particular clauses the BPTO will not approve: the Brazilian Patent and Trademark Office (BPTO), . . . does not authorize clauses (i) limiting the use of the know-how, even after the termination of the agreement, (ii) of unlimited confidentiality term, and (iii) requesting devolution of materials from the licensor, for example. The interpretation of the BPTO is that technology not protected by a patent can only be "transferred" to a Brazilian party rather than "licensed", therefore, the trade secret may be assigned ("sold"), but not "licensed". [36] An expert report notes the following issues with Brazilian trade secret law:[37] 1) First: As mentioned above in answer 7, the contractual aspects regarding trade secrets may be considered a very important issue for Brazil. BPTO's interpretation that trade secrets cannot be licensed creates practical limitations (i.e. for the contract drafting and, subsequently, for the ability of the holder to control its use) when the agreements are subject to registration before such office. Court decisions from the eighties (80's) accepted BPTO's unlimited competence for this interpretation. Currently, certain sparse decisions criticizing BPTO's policies when registering agreements were rendered, but one cannot yet assert that there is a final/definite case law orientation about this issue or even that there is a significant volume of precedents. Therefore, it is needed for improvement of the Brazilian system that a clear definition be adopted by the Courts on the possibility of trade secret to be licensed in Brazil and, eventually, new policies or interpretations of the BPTO be adopted accepting this position, or at least formulating an official guideline on its policies on this subject, to be used by contractual parties. 2) Second: Violation of trade secrets (and of Industrial Property rights in general) is treated by our statutory law as a "crime of lower offensive potential". Penalties

35 MacLaren, Trade Secrets Throughout the World § 5:8 (2012).

36 Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, Brazil 7 (2010),

37 Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, Brazil 9 - 10 (2010).

foreseen are low ("detention of 3 (three) months to 1 (one) year) or a fine") and their lack of effectiveness together with the difficulties to recover damages create relative values and enforcement difficulties.

3) Third: Although injunctions are rendered, the slowness of our Judiciary system is often incompatible with trade secret dynamics.3) Third: Although injunctions are rendered, the slowness of our Judiciary system is often incompatible with trade secret dynamics.

4) Fourth: Trade secret protection has evolved and improved in our country, but there is less awareness of its protection in the public sector and one still sometimes finds judges that require the presentation of the "registration" of the secret.

5) Fifth: Experts' reports and evidence in general are often difficult obstacles to overcome in trade secret litigation and deserve more study and development.

6) Sixth: Improvements for the protection of trade secrets during litigation are desired.

7) Seventh: Our Customs authorities are not prepared nor equipped to evaluate trade secrets violations in case of necessity to apply retention measures (answer 5 above).

The US pharmaceutical trade association, PhRMA has criticized Brazil's data protection policies:

The Brazilian Government still adopts a flexible interpretation of Article 39 of the TRIPS Agreement to allow Government officials to grant marketing approval relying on test and other data submitted by our member companies to prove the safety and efficacy of their products. While some positive steps have been taken to prevent inappropriate disclosure of these data held by the Government, additional efforts are needed to provide certainty that test and other data will be protected fully against unauthorized use to secure marketing approval for a fixed period of time. Our member companies continue efforts to gain protection for their data through the Judiciary System, with limited success. The intense debate in the Judiciary demonstrates the lack of clarity in the Brazilian legal framework regarding RDP protection for pharmaceuticals. Although federal law 10.603/02 provides adequate protection for veterinary and crop products, the Brazilian legislation still does not provide a similar benefit for pharmaceutical products, resulting in discriminatory treatment. A productive dialogue among U.S. and Brazilian authorities could lead to an appropriate RDP regime for pharmaceutical products in Brazil by assuring that the domestic legislation meets high standards. In conclusion, Brazil lacks sufficient protection for data submitted for innovative biopharmaceutical products. A period of data protection preventing ANVISA from relying on the innovator's data in approving a follow-on medicine application is needed. Although there have been lawsuits seeking to secure a period of data protection for specific products, so far the Courts are split, leaving innovators without reliable regulatory data protection.[38]

SOURCES:

MacLaren, Trade Secrets Throughout the World § 5 (2012).
Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, Brazil (2010).

[38] PhRMA Special 301 Submission 2013 at 85 – 86, available at http://www.phrma.org/sites/default/files/pdf/PhRMA%20Special%20301%20Submission%202013.pdf.

BULGARIA

Source of Law, Definition and Scope

Statutory or Other Protection		**Definition**			**Additional Elements of Definition**					**Scope**	
Civil	Criminal	All confidential business information	Common Definition: Confidential business information, **subject to:** deriving value from secrecy; reasonable and making reasonable efforts to maintain secrecy.	Common definition **plus condition that** it be imparted to recipient in confidence	Use must be shown	Inventory of trade secrets required	Must be reduced to writing	Must be identified as a trade secret to recipient	Written notice to recipient required	Confidential Business Information	Technical Information
No single source of comprehensive statutory protection, but effectively comprehensive protection spread across statutes.	No. (Beyond certain very isolated and specific offenses).	No.	Yes.	No.	No.	No.	No.	Yes.	Perhaps.	Yes.	Yes.

BULGARIA

Covered Acts

Acts Covered as Civil Infringement		**Acts Covered as Crimes**		**Third Parties:** **Liable for Acquisition?** **Liable Even if Innocent (Without Knowledge)?**	
Breach of Duty?	Wrongful Acquisition/ Misappropriation	Breach of Duty?	Wrongful Acquisition/ Misappropriation	Civil	Criminal
Use in Breach of Duty. Disclosure in Breach of Duty.	Yes.	No.	No.	Yes. No. Knowledge or reason to know required.	Not applicable.

BULGARIA

Defining Duties and Misappropriation

Defining Duty of Confidentiality			**Restrictions on Duty of confidentiality**		**Defining Wrongful Acquisition - Misappropriation**	
Commercial Relationship	Current Employment Relationship	Past Employment Relationship	Commercial Relationship	Employment Relationship	Civil	Criminal
Duty can be based on express agreement in commercial contract. Duty can be implied in the context of a business relationship.	Duty can be based on express agreement. Duty is statutorily imposed in the context of an employment relationship.	Uncertain.	Generally valid.	Uncertain.	Torts, crimes, and other violations of good faith commercial practices. May be difficult to prove. See comments below.	Not applicable.

BULGARIA

Restrictions on Liability

Additional Elements of Proof in Infringement Claim		**Contractual Restrictions on Competition - Validity**		**Defences**	
Civil	Criminal	Commercial Relationship	Post-Employment	Civil	Criminal
None.	Not applicable.	Enforceable, subject to competition law.	Invalid and unenforceable.	Independent creation. Reverse engineering.	Not applicable.

BULGARIA

Remedies

Civil Remedies								**Criminal Remedies**		
Preliminary injunction	Permanent injunction	Injunction to eliminate wrongful head start	Delivery up and/or destruction of infringing materials	Compensatory Damages – Availability and Type	Defendant's Profits	Punitive damages available?	Statutory or Pre-established damages	Fines	Jail Sentence	Other
Yes. Bond typically required.	Yes, in fact, but not specifically provided for. Specific enforcement of contracts.	No.	No.	Direct damages Loss of profit. If defendant breached a contract in bad faith, proximate damages also available.	No.	No.	No.	None.	None.	None.

BULGARIA

Enforcement, investigation and discovery & related regulations

Enforcement, investigation and discovery			**Data Exclusivity**		**Technology Transfer**	**Legal Complements**
Emergency Search to preserve and obtain proof	Pre-trial discovery	Protection of confidentiality of trade secrets in litigation	Drugs	Agricultural Chemicals		Fraser Score
Yes. Ex parte available. An official conducts search.	Documentary under supervision of court. No sanction for failure to comply, other than adverse inference drawn by court.	Closed hearing available, although open to parties and agents. Protection from other party may be available.	"8 + 2 + 1 year approach." Pharmaceutical test data submitted to government for new medicinal products and new indications or uses is protected from disclosure or use for 8 years. Once the 8 year period ends, the data can be used by generic manufacturers to prepare and apply for regulatory approval, but not market a product. This period of market exclusivity lasts 2 years. The initial applicant may receive another 1 year for new indications.	"8 + 2 + 1 year approach." Test data submitted to government for new products and new indications or uses is protected from disclosure or use for 8 years. Once the 8 year period ends, the data can be used by generic manufacturers to prepare and apply for regulatory approval, but not market a product. This period of market exclusivity lasts 2 years. The initial applicant may receive another 1 year for new indications.	None.	On the Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, Bulgaria receives a score of 5.0 out of 10, which ranks it 90th in the world.[39] It scores particularly low on judicial independence (3.2 out of 10) and impartial courts (2.9).

[39] Fraser Institute, Economic Freedom of the World 2012 Annual Report (2012).

BULGARIA

Additional Comments

Expert characterisation of the operation of the protection of trade secrets in practice
Limited number of cases have been brought. Four in 2011; four in 2010; one in 2009.[40] An expert report observes that proving the existence of a trade secret may be difficult. Courts require that they have been identified with specificity to recipients, perhaps in writing and pursuant to an agreement:[41] The most common difficulty observed is the enforcement of trade secrets in commercial relations - trade secrets disclosed between counterparties in the course of distribution agreements, agency, etc. As the definition of a trade secret under the Law on Protection of Competition requires protective measures to be undertaken to secure a trade secret, lack or insufficiency of such protection measures may preclude given information to be seen as a trade secret. Courts are particularly demanding in their examination whether protective measures have been implemented. Staff regulations imposing an obligation on employees not to disclose confidential information and to protect the good standing of their employer were found to be too general and blank to be deemed to protect trade secrets. Protective measures shall specifically identify trade secrets as such. In this respect, lack of adequate protection measures prevents information to be classified and accordingly protected as a trade secret. In the court's case law, examples of protection measures include company's staff regulations prohibiting misuse and disclosure of trade secrets, internal orders classifying information as a trade secret, confidentiality clauses in employment agreements, technical protection devices, differentiated levels of access to information database, etc. Misappropriation is also difficulty to prove:[42] The regulatory authority and courts have demonstrated their reluctance to accept trade secrets abuse unless there is very strong and unequivocal evidence proving such abuses beyond any doubt.

SOURCES:

Hogan Lovells Report (2012).

40 Hogan Lovells Report, Appendix 3 at 15 (2012).

41 Ibid at 16.

42 Ibid.

CHINA

Source of Law, Definition and Scope

Statutory or Other Protection		**Definition**			**Additional Elements of Definition**					**Scope**	
Civil	Criminal	All confidential business information	Common Definition: Confidential business information, **subject to:** deriving value from secrecy; reasonable and making reasonable efforts to maintain secrecy	Common definition **plus condition that** it be imparted to recipient in confidence	Use must be shown	Inventory of trade secrets required	Must be reduced to writing	Must be identified as a trade secret to recipient	Written notice to recipient required	Confidential Business Information	Technical Information
Compre-hensive civil protection pursuant to statute.	Compre-hensive criminal protection pursuant to statute. Additional administrative enforcement by the State Administration for Industry and Commerce.	No.	Yes.	No.	No.	No.	Not de jure, but de facto, yes, at least in breach of duty cases. Commentators recommend written agreements and acknowledge-ment of receipt due to evidentiary concerns.	Not de jure, but de facto, yes, at least in breach of duty cases. Commentators recommend written agreements and acknowledge-ment of receipt due to evidentiary concerns.	Not de jure, but de facto, yes, at least in breach of duty cases. Comment-ators recommend written agreements and acknowledge-ment of receipt due to evidentiary concerns.	Yes.	Yes.

CHINA

Covered Acts

Acts Covered as Civil Infringement		**Acts Covered as Crimes**		**Third Parties:** **Liable for Acquisition?** **Liable Even if Innocent (Without Knowledge)?**	
Breach of Duty?	Wrongful Acquisition/ Misappropriation	Breach of Duty?	Wrongful Acquisition/ Misappropriation	Civil	Criminal
Yes.	Yes.	Yes.	Yes.	Yes. No. Only liable if third party has knowledge or reason to know.	Yes. No. Only liable if third party has knowledge or reason to know.

CHINA

Defining Duties and Misappropriation

Defining Duty of Confidentiality			**Restrictions on Duty of confidentiality**		**Defining Wrongful Acquisition - Misappropriation**	
Commercial Relationship	Current Employment Relationship	Past Employment Relationship	Commercial Relationship	Employment Relationship	Civil	Criminal
Duty effectively must be based on express agreement (except in the case of a failed contract negotiation). Duty not to disclose or use.	Duty effectively must be based on express agreement only. Duty not to disclose or use.	Duty can be based on express agreement only. Ends with public disclosure.	Ends with public disclosure of confidential information.	Ends with public disclosure of confidential information.	Acquiring a trade secret by illegal or tortious acts, inducement of breach of duty, and other improper means, as well as disclosing, using, or allowing others to use a trade secret obtained by illegal or improper means. The catch-all category of "improper means" is not defined in the Act or subsequent interpretations, but potentially broad – it may apply to all unauthorized acquisition other than independent creation or reverse engineering.	Same as civil, but also requires "serious" or "exceptionally serious" losses.

CHINA

Restrictions on Liability

Additional Elements of Proof in Infringement Claim		**Contractual Restrictions on Competition - Validity**		**Defences**	
Civil	Criminal	Commercial Relationship	Post-Employment	Civil	Criminal
The difficulty in proving the existence of trade secrets leads experts to recommend: (1) a written agreement with any recipients; (2) specific identification of the trade secret in writing; and (3) written acknowledgement of receipt.	The difficulty in proving the existence of trade secrets leads experts to recommend: (1) a written agreement with any recipients; (2) specific identification of the trade secret in writing; and (3) written acknowledgement of receipt.	Permissible only if pro-competitive benefits outweigh harms.	Enforceable only with respect to senior management, senior technical personnel, and employees who had a confidentiality obligation. They must specify monthly compensation for the term of the non-compete. The period may not exceed two years after employment.	Independent creation. Reverse engineering.	Independent creation. Reverse engineering.

CHINA

Remedies

Civil Remedies								**Criminal Remedies**		
Preliminary injunction	Permanent injunction	Injunction to eliminate wrongful head start	Delivery up and/or destruction of infringing materials	Compensatory Damages – Availability and Type	Defendant's Profits	Punitive damages available?	Statutory or Pre-established damages	Fines	Jail Sentence	Other
Not in fact according to expert opinion.	Yes. (For so long as remains secret).	Uncertain.	Yes.	General compensatory damages. Lost profits. Consequential damages. Reasonable royalty.	Yes.	No.	No.	Available but unspecified in criminal proceedings. In administrative proceedings, fines of between RMB 10 000 and RMB 200 000.	"Serious" losses of RMB 500 000 or more incur a jail sentence of up to three years. "Exceptionally serious" losses of RMB 2 500 000 or more warrant a sentence of three to seven years.	Return of materials and destruction of products made with trade secret.

CHINA

Enforcement, investigation and discovery & related regulations

Enforcement, investigation and discovery			**Data Exclusivity**		**Technology Transfer**	**Legal Complements**
Emergency Search to preserve and obtain proof	Pre-trial discovery	Protection of confidentiality of trade secrets in litigation	Drugs	Agricultural Chemicals		Fraser Score
Yes. Conducted by judge. Commonly granted. Ex parte available.	None.	Partial protection with respect to hearings (in camera hearings available, but not fully closed). Protection of documents. No protection from other party and its agents.	Six years from date of marketing approval. Largely moot because regulatory approval will be granted based on approvals in foreign countries and summary data published in those countries.	Six years from date of marketing approval.	Registration of technology import agreements required, but not approval (except for certain restricted technologies). Employees must be separately compensated for technology they develop and have right-of-first refusal for transfer or license. Substantive regulations on contents of technology import agreements, which largely do not affect trade secrets.	On the Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, China receives a score of 6.2 out of 10, which ranks it 49th in the world.[43] It lowest scores are with respect to judicial independence (4.9 out of 10) and impartial courts (5.2 out of 10).[44]

43 Fraser Institute, Economic Freedom of the World 2012 Annual Report (2012).

44 Ibid.

CHINA

Additional Comments

Expert characterisation of the operation of the protection of trade secrets in practice
Comments from the business sector reflect poor perceptions regarding how well China protects trade secrets within China. In 2009, the security firm McAfee surveyed "1 000 senior IT decision makers in the US, UK, Japan, China, India, Brazil and the Middle East."[45] The report found that about 50% of respondents rated the "threat level" to their sensitive data in China as "high."[46] The report related the following perceptions: Three countries, in particular, stood out to the survey respondents—perhaps reflecting broader security perceptions. Respondents cited China, Pakistan and Russia as the worst-rated countries when it comes to the protection of digital assets. Pakistan, China and Russia, in that order, were also perceived to have the worst reputations for pursuing or investigating security incidents. Respondents cited corruption among law enforcement and the legal systems as well as poor skills among law enforcement as top reasons for the reputation rating.[47] The report also found that over 25% of respondents had avoided doing business in China due to security concerns.[48] A 2011 survey of international business executives by McAfee and SAIC found these concerns about China unabated, as survey respondents once again ranked China among the top three security threats and among the top three countries where they avoided doing business due to security threats.[49] Several governments have expressed grave concerns about theft of trade secrets originating from China. In February 2013, the Executive Office of the President of the United States released a report on trade secret theft entitled "Administration Strategy on Mitigating the Theft of U.S. Trade Secrets."[50] In addition to setting forth a strategy, the report gathered several previous U.S. government assessments of the trade secret problem, including a 2011 report by the Office of the National Counterintelligence Executive.[51] This report identifies China as a posing a "pervasive threat" as one of the two most "aggressive collectors" (the other one identified was Russia) "of U.S. economic information and technology."[52] In the days and weeks that followed release of the Administration Strategy, senior U.S. officials frequently promoted the strategy

45 McAfee, Unsecured Economies: Protecting Vital Information 1, 2 (2009).

46 McAfee, Unsecured Economies: Protecting Vital Information 1, 12 (2009).

47 McAfee, Unsecured Economies: Protecting Vital Information 1, 13 (2009).

48 McAfee, Unsecured Economies: Protecting Vital Information 1, 14 (2009).

49 McAfee, Underground Economies: Intellectual Capital And Sensitive Corporate Data Now The Latest Cybercrime Currency 10 (2011).

50 Executive Office of the President of the United States, Administration Strategy on Mitigating the Theft of U.S. Trade Secrets (February 2013).

51 Office of the National Counterintelligence Executive Report, Foreign Spies Stealing US Economic Secrets in Cyberspace (2011).

52 Ibid at 4 - 5.

and cited China (along with Russia) as a threat. Other governments have similarly singled out China as a source of trade secret theft.[53] For example, the head of Germany's military intelligence stated that one of his agency's main priorities was combatting industrial espionage from China and Russia.[54]

Reports and accusations of trade secret theft emanating from China have grown more specific in recent months as the U.S. government has adopted a "naming and shaming" policy. For example, on 19 May 2013, the New York Times reported that Unit 61398, a "cyber unit" of China's People's Liberation Army based in Shanghai had resumed attacks that "had stolen data from scores of American companies and government agencies."[55] According to the Times:

> The hackers were behind scores of thefts of intellectual property and government documents over the past five years, according to a report by [a security firm] in February that was confirmed by American officials. They have stolen product blueprints, manufacturing plans, clinical trial results, pricing documents, negotiation strategies and other proprietary information from more than 100 of [the security firm's] clients, predominantly in the United States. According to security experts, the cyber unit was responsible for a 2009 attack on the Coca-Cola Company that coincided with its failed attempt to acquire the China Huiyuan Juice Group.

Commentary by Chinese experts is far more sanguine than the foreign perspective, but ultimately concedes and demonstrates the practical difficulty of proving a trade secret infringement claim and how it undermines the effectiveness of trade secret law in China. One expert commentary is typical. While acknowledging certain difficulties in enforcement, the commentators offered generally positive views:

> Over the past two decades, China has developed a comprehensive set of laws, regulations, and judicial interpretations designed to protect the rights of trade secret owners. Enforcement of trade secrets, however, is not straightforward. This is primarily because China does not have a US-style discovery system, and the evidentiary burden for a plaintiff to bring a trade secret misappropriation case in Chinese courts is relatively high. Notwithstanding the difficulties, there have been numerous cases of successful enforcement, both civil and criminal. Experience shows that it is possible to protect and enforce trade secrets in China, but the devil is in the details.[56]

Nevertheless, gathering evidence and proving a case appears to be difficult. These same commentators observed the difficulty of providing proof sufficient to obtain a preliminary injunction, which is typically considered essential in a trade secret case:

> Unlike a patent, trademark, or copyright, a trade secret is not a right granted by a government agency. Whether something constitutes a trade secret is almost always subject to disputes. As such, the likelihood of success on the merits is more difficult to prove for trade secret cases. Moreover, China has not adopted the inevitable disclosure doctrine. Therefore, it is rather unusual to obtain a preliminary injunction for trade secret misappropriation.[57]

---

53 Ibid at Appendix B-1.

54 Reuters, *German Spy Chief Targets Russian, Chinese Industrial Espionage*, 18 February 2013, http://www.reuters.com/article/2013/02/18/us-germany-spies-idUSBRE91H08C20130218

55 David Sanger & Nicole Perlroth, "Chinese Hackers Resume Attacks on U.S. Targets," New York Times, A1, 19 May 2013, http://www.nytimes.com/2013/05/20/world/asia/chinese-hackers-resume-attacks-on-us-targets.html?_r=0.

56 Benjamin Bai & Guoping Da, Strategies for Trade Secrets Protection in China, 9 Northwestern Journal of Technology and Intellectual Property 351, 374-375 (2011).

57 Ibid at 361.

Another commentator described the great difficulty in proving a trade secret case in China:

> The evidentiary requirements for court actions in China are very stringent. Little weight is generally accorded to affidavits and witness testimonies while physical evidence and documentary evidence are favoured. Such evidence is difficult to obtain in trade secret infringement cases. This problem is compounded by the problems relating to the lack of a discovery process in the PRC. In the PRC system, each party needs to adduce sufficient evidence to prove its claims. Although the court has the power to assist parties to gather evidence, such power is rarely used. Particularly when a rightholder is trying to gather evidence of infringement from an established infringer where it is often difficult to gain entry, there may be undue hardship for the rightholder.[58]

As previously noted, injunctions are available, but it is unusual to obtain one in a trade secret case, and they are thus, in effect, unavailable.[59] One expert observes the following:

> However, in cases involving trade secrets and other intellectual properties, the applicability of the preliminary [injunction] is weak and its application is very limited in such cases. This is mainly because the conditions for preliminary execution are hard to meet in law suits involving trade secrets. Article 98(1) of the Civil Procedure Law provides that cases in which preliminary execution is ordered by the people's court shall meet the condition that the relationship of rights and obligations between the parties is definite, and that denial of preliminary execution would seriously affect the life or business of the applicant. This requires the applicant and the judge to explain, in order to support the adoption of a preliminary execution order, why, in the absence of such order, the production or business operation of the applicant will be seriously affected. However, cases involving trade secrets are often complicated. The parties have substantial disagreements on whether the trade secret of the plaintiff exists, whether the defendant's activity has been based on such trade secret or just on common knowledge, experience and skills of the defendant, etc. The rights and obligations between the plaintiff and the defendant are not clear. Furthermore, a lot of trade secrets cost little to form, contain little originality, are often not in use or belong to negative information, which, even if used by others, will not seriously affect the life or business of the right holder. Therefore, it is difficult for the plaintiff to apply for preliminary execution in these cases.[60]

There is no ordinary pre-trial discovery available to plaintiffs in civil cases. This lack of discovery poses a great difficulty for plaintiffs, particularly given the preference of Chinese courts for original, documentary evidence over testimony and affidavits.[61] One expert opinion observes the effects:

> Because there is no U.S.-style discovery in China, plaintiffs must collect and submit their own evidence to meet their burden of proof regarding, inter alia, trade secret misappropriation and damages. Chinese courts rarely accept evidence unless in its original form; therefore, documentary evidence is practically the only form of evidence that carries significant weight in a Chinese court. However, evidence obtained in violation of law is inadmissible in Chinese courts, and if admitted, it may constitute reversible error on appeal. Subsequently, it is essential to have a proper and thorough evidence gathering strategy to overcome the challenging evidentiary hurdles for a

58 Terrence F. MacLaren, Chiang Ling Li, 1 Trade Secrets Throughout the World § 8.52 (2012) (hereafter "MacLaren, Trade Secrets Throughout the World").

59 Ibid; Shan Hailing, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, China 34 - 35 (2010), available at: https://www.aippi.org/download/commitees/215/GR215china.pdf.

60 Shan Hailing, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, China 35 (2010), available at: https://www.aippi.org/download/commitees/215/GR215china.pdf.

61 MacLaren, Trade Secrets Throughout the World § 8.52 (2012).

> potential plaintiff in a trade secret misappropriation case. In some cases, it is challenging to obtain documentary evidence to prove misappropriation. In others, it may be difficult to prove that the potential defendant had access to confidential information.[62]

These evidentiary challenges lead experts to consistently recommend confidentiality agreements as absolutely necessary to protect trade secrets.[63] As noted above, such agreements are also advised due to the (likely insurmountable) difficulty of obtaining a preliminary injunction, where "the relationship of rights and obligations between the parties [must be shown to be] definite."[64] However, even a written agreement is likely not enough:

> As a practical result, though trade secrets can be protected by means similar to those used in the US, such as a confidentiality agreement, the mere existence of a confidentiality agreement may not be sufficient. It is advisable to have the recipient sign an acknowledgement of receiving access to the confidential information, in addition to executing a confidentiality agreement, prior to giving confidential information to a recipient.[65]

Thus, not only is pre-trial discovery non-existent for trade secret cases, but evidentiary burdens are extremely high, making it difficult to prove a case.
Criminal prosecutions may be difficult to obtain. One authority notes:

Generally speaking, criminal prosecution is very effective in trade secret misappropriation cases, but it is not always easy to get police interested in run-of-the-mill trade secret cases. In the authors' experiences, the police are more interested in high profile cases. Consequently, the authors advise that one should try to "package" the case as "high profile" to enhance the chance of criminal prosecution. It also is important to build good relationships with the local community, including the local police, before any misappropriation happens.[66]

SOURCES:

See Annex 2 of this paper for a detailed overview of China's trade secret law and sources.

---

62 Benjamin Bai & Guoping Da, Strategies for Trade Secrets Protection in China, 9 Northwestern Journal of Technology and Intellectual Property 351, 362 - 363 (2011).

63 See ibid; MacLaren, Trade Secrets Throughout the World § 8.7 (2012); Shan Hailing, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, China 10, 27, 34 (2010), available at https://www.aippi.org/download/commitees/215/GR215china.pdf.

64 Shan Hailing, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, China 35 (2010), available at https://www.aippi.org/download/commitees/215/GR215china.pdf.

65 Benjamin Bai & Guoping Da, Strategies for Trade Secrets Protection in China, 9 Northwestern Journal of Technology and Intellectual Property 351, 363 (2011).

66 Benjamin Bai & Guoping Da, Strategies for Trade Secrets Protection in China, 9 Northwestern Journal of Technology and Intellectual Property 351, 365 (2011).

COLOMBIA

Source of Law, Definition and Scope

Statutory or Other Protection		**Definition**			**Additional Elements of Definition**					**Scope**	
Civil	Criminal	All confidential business information	Common Definition: Confidential business information, **subject to:** deriving value from secrecy; reasonable and making reasonable efforts to maintain secrecy	Common definition **plus condition that** it be imparted to recipient in confidence	Use must be shown	Inventory of trade secrets required	Must be reduced to writing	Must be identified as a trade secret to recipient	Written notice to recipient required	Confidential Business Information	Technical Information
Yes.	Yes.	No.	Yes.	No.	No.	No.	No.	No.	No.	Yes.	Yes.

COLOMBIA

Covered Acts

Acts Covered as Civil Infringement		**Acts Covered as Crimes**		**Third Parties:** **Liable for Acquisition?** **Liable Even if Innocent (Without Knowledge)?**	
Breach of Duty?	Wrongful Acquisition/ Misappropriation	Breach of Duty?	Wrongful Acquisition/ Misappropriation	Civil	Criminal
Use in Breach of Duty. Disclosure in Breach of Duty.	Yes.	Yes.	Yes.	Yes. No. Knowledge required.	Yes. No. Knowledge required.

COLOMBIA

Defining Duties and Misappropriation

Defining Duty of Confidentiality			**Restrictions on Duty of confidentiality**		**Defining Wrongful Acquisition - Misappropriation**	
Commercial Relationship	Current Employment Relationship	Past Employment Relationship	Commercial Relationship	Employment Relationship	Civil	Criminal
Duty can be based on express agreement in commercial contract. Duty can be implied in the context of a business relationship.	Duty can be based on express agreement. Duty is statutorily imposed in the context of an employment relationship.	Express duty is enforceable.	None.	None.	To "unlawfully gains knowledge of, copies, or obtains a secret". To "internally destabilize a competitor, or to unfairly obtain its secret". Misappropriation of documents containing secrets.	To "unlawfully gains knowledge of, copies, or obtains a secret". To "internally destabilize a competitor, or to unfairly obtain its secrets". Misappropriation of documents containing secrets.

COLOMBIA

Restrictions on Liability

Additional Elements of Proof in Infringement Claim		**Contractual Restrictions on Competition - Validity**		**Defences**	
Civil	Criminal	Commercial Relationship	Post-Employment	Civil	Criminal
None.	Not applicable.	Enforceable, subject to competition law.	Valid for up to two years.	Independent creation. Reverse engineering.	Independent creation. Reverse engineering.

COLOMBIA

Remedies

Civil Remedies								**Criminal Remedies**		
Preliminary injunction	Permanent injunction	Injunction to eliminate wrongful head start	Delivery up and/or destruction of infringing materials	Compensatory Damages – Availability and Type	Defendant's Profits	Punitive damages available?	Statutory or Pre-established damages	Fines	Jail Sentence	Other
Yes. Takes about two months to obtain.	Yes.	No.	No.	Actual losses. Loss of profit.	No.	No.	No.	10 000 to 300 000 pesos. 500 000 if profit is obtained.	1 to 5 years. 1.5 to 6 years if profit is obtained.	None.

COLOMBIA

Enforcement, investigation and discovery & related regulations

Enforcement, investigation and discovery			**Data Exclusivity**		**Technology Transfer**	**Legal Complements**
Emergency Search to preserve and obtain proof	Pre-trial discovery	Protection of confidentiality of trade secrets in litigation	Drugs	Agricultural Chemicals		Fraser Score
No.	Documentary and interrogatories under supervision of court.	None.	Five years from approval for new chemical components.	Five years from approval for new chemical components.	Employer owns employee inventions, but employee has right to compensation for their use. Inbound agreements subject to approval, but approval will be automatically approved if there is no objection within 15 days. Substantive restrictions involving trade secrets: No prohibitions on price or volume of production; no requirement to assign improvements or other inventions. No royalties for technology contributed to joint venture.	On the Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, Colombia receives a score of 4.4 out of 10, which ranks it 110th in the world.[67] It scores particularly low on enforcement of contracts (2.1 out of 10).

67 Fraser Institute, Economic Freedom of the World 2012 Annual Report (2012).

COLOMBIA

Additional Comments

Expert characterisation of the operation of the protection of trade secrets in practice
There is extremely limited expert commentary on Colombian Trade Secret Law. "There is essentially no jurisprudence directly covering the criminal acts relating to trade secrets."[68]

SOURCES:

MacLaren, Trade Secrets Throughout the World § 9 (2012).

[68] MacLaren, Trade Secrets Throughout the World § 9:4 (2012).

FRANCE

Source of Law, Definition and Scope

Statutory or Other Protection		**Definition**			**Additional Elements of Definition**					**Scope**	
Civil	Criminal	All confidential business information	Common Definition: Confidential business information, **subject to:** deriving value from secrecy; reasonable and making reasonable efforts to maintain secrecy	Common definition **plus condition that** it be imparted to recipient in confidence	Use must be shown	Inventory of trade secrets required	Must be reduced to writing	Must be identified as a trade secret to recipient	Written notice to recipient required	Confidential Business Information	Technical Information
No comprehensive civil protection pursuant to specific statute. Protection by means of various laws of general applicability against unfair competition.	No comprehensive criminal protection. Some isolated trade secret-specific protection in particular situations and also by means of various laws of general applicability.	No.	Yes. Substantial, secret, and provides a competitive advantage.	No.	No	No.	No.	No.	No.	Yes; also a category of know how.	Yes, (Defined as “manufacturing secrets”).

FRANCE

Covered Acts

Acts Covered as Civil Infringement		**Acts Covered as Crimes**		**Third Parties:** **Liable for Acquisition?** **Liable Even if Innocent (Without Knowledge)?**	
Breach of Duty?	Wrongful Acquisition/ Misappropriation	Breach of Duty?	Wrongful Acquisition/ Misappropriation	Civil	Criminal
Yes. Breach of contract by employees or other contracting parties. Disclosure by employees or managers in breach of implied duty.	Yes, but not comprehensive. See definition below.	Yes. **Disclosure** of **manufacturing secrets** in breach of duty by an employee or manager.[69] **Disclosure** or **use** of **confidential business information, technical information or know how**, in breach of trust, where one has been entrusted with information – most likely pursuant to an agreement, or implicitly in case of employees, agents, or professionals.[70] Professionals (e.g., doctors, lawyers) are also liable for breach of duty for disclosing any confidential information.[71]	Generally not applicable, except where a party steals physical media or commits some other related wrongful act.	Yes, where the third party induces an employee or manager to reveal a trade secret by bribing them or hiring them. No. Only liable if third party has knowledge and wilfully engages in bribery or hiring the employee with the object of obtaining the trade secret.	Yes –knowing receipt of stolen information. Knowledge required.

69 Article L. 1227-1 of the Labor Code and Article L. 621-11 of the Intellectual Property Code.

70 Art 314-1 of the Criminal Code.

71 Art. 226-13 of the Criminal Code.

FRANCE

Defining Duties and Misappropriation

Defining Duty of Confidentiality			**Restrictions on Duty of confidentiality**		**Defining Wrongful Acquisition - Misappropriation**	
Commercial Relationship	Current Employment Relationship	Past Employment Relationship	Commercial Relationship	Employment Relationship	Civil	Criminal
Duty can be based on express agreement in commercial contract. Not implied.	Duty can be based on express agreement and implied duty.	Duty can be based on express contract. Duty is also implied. Implied duty narrower after employment – only trade secrets. No inevitable disclosure doctrine.	None.	Express agreements and implied post-employment duties to keep information confidential likely unenforceable with respect to general skills and knowledge.	The theft of documents containing a trade secret. Bribing or paying a competitor's employees. The unfair hiring away of a competitor's employees with a view to obtaining trade secrets. Use of a wrongfully-obtained secret. Apparently not eavesdropping or circumvention of security where no other unlawful act is committed.	Not applicable.

FRANCE

Restrictions on Liability

Additional Elements of Proof in Infringement Claim		**Contractual Restrictions on Competition - Validity**		**Defences**	
Civil	Criminal	Commercial Relationship	Post-Employment	Civil	Criminal
None.	None.	Commercial agreements not to compete generally enforceable.	Courts reluctant to enforce if negatively affect ability to earn a living. Post-employment agreements not to compete enforceable if reasonable with respect to competitive need, time and geographic scope.	Independent creation. Reverse engineering. Potential of reverse engineering negates secrecy.	Independent creation. Reverse engineering. Potential of reverse engineering negates secrecy.

FRANCE

Remedies

Civil Remedies								**Criminal Remedies**		
Preliminary injunction	Permanent injunction	Injunction to eliminate wrongful head start	Delivery up and/or destruction of infringing materials	Compensatory Damages – Availability and Type	Defendant's Profits	Punitive damages available?	Statutory or Pre-established damages	Fines	Jail Sentence	Other
Yes. But rarely granted – see additional comments below.	Yes. (For so long as remains secret). But rarely granted – see additional comments below.	No.	Yes.	Out of pocket. Lost Profits. Consequential. Legal fees. Moral damages (loss of reputation).	No.	No.	No.	Disclosure of manufacturing secrets up to 30 000 Euros. Breach of trust up to 375 000 Euros.	Disclosure of manufacturing secrets up to 2 years. Breach of trust up to 3 years.	A third party who receives stolen information can be punished under Article 321-1 of the Criminal Code with 5 years of imprisonment and a 375 000 Euro fine.

FRANCE

Enforcement, investigation and discovery & related regulations

Enforcement, investigation and discovery			**Data Exclusivity**		**Technology Transfer**	**Legal Complements**
Emergency Search to preserve and obtain proof	Pre-trial discovery	Protection of confidentiality of trade secrets in litigation	Drugs	Agricultural Chemicals	Civil	Fraser Score
Yes. Ex parte available. Conducted under direction of court, not parties.	Documentary. Conducted under direction of court, not parties.	Limited. In camera hearings available only if all parties agree. No protection from other party available unless court issues an extraordinary order. Final judgment must be fully publically accessible.	"8 + 2 + 1 year approach." Pharmaceutical test data submitted to government for new medicinal products and new indications or uses is protected from disclosure or use for 8 years. Once the 8 year period ends, the data can be used by generic manufacturers to prepare and apply for regulatory approval, but not market a product. This period of market exclusivity lasts 2 years. The initial applicant may receive another 1 year for new indications.	"8 + 2 + 1 year approach." Pharmaceutical test data submitted to government for new medicinal products and new indications or uses is protected from disclosure or use for 8 years. Once the 8 year period ends, the data can be used by generic manufacturers to prepare and apply for regulatory approval, but not market a product. This period of market exclusivity lasts 2 years. The initial applicant may receive another 1 year for new indications.	None.	On the Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, France receives a score of 7.31 out of 10, which ranks it 26th in the world.

FRANCE

Additional Comments

Expert characterisation of the operation of the protection of trade secrets in practice
A recent parliamentary report noted, "legislation relative to unfair competition applies only in conditions which are difficult to bring together and which are not particularly restrictive for violators."[72] In the view of the report authors, French trade secret protection is not seen as being effective: > there have been relatively few examples of case law over the past decade and, in case of conviction, but for exceptions, the penalties which are imposed are limited to modest damages; prohibition of use is quite rare. . . . This might lead one to think that the protection of trade secrets in France would not generally be very effective.[73] A commentator also remarks that greater protection during litigation is desired: > The difficulties of ensuring the preservation of the secrets of one or more parties to a proceeding and, in particular, the difficulty of getting the judge to order a measure of confidentiality prohibiting the parties from disclosing to third parties the documents transmitted, the obligation, in order to obtain closed proceedings, for this to be requested by all the parties, and the impossibility for the judge to limit access to judgements or to draft several versions of his judgement (a confidential version for the parties and an expurgated version which would be the only one accessible to third parties).[74] A report notes that courts rarely grant preliminary and permanent injunctions: "But from analysis of French case law in this field, it emerges that injunctions are rarely ordered and that only damages are usually granted."[75]

SOURCES:

See Annex 2 of this paper for a detailed overview of France's trade secret law and sources.

72 Jean-Pierre Stouls et al., Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, France 1 (2010).

73 Ibid.

74 Ibid at 25.

75 Ibid at 13.

GERMANY

Source of Law, Definition and Scope

Statutory or Other Protection		**Definition**			**Additional Elements of Definition**					**Scope**	
Civil	Criminal	All confidential business information	Common Definition: Confidential business information, **subject to:** deriving value from secrecy; reasonable and making reasonable efforts to maintain secrecy	Common definition **plus condition that** it be imparted to recipient in confidence	Use must be shown	Inventory of trade secrets required	Must be reduced to writing	Must be identified as a trade secret to recipient	Written notice to recipient required	Confidential Business Information	Technical Information
Not comprehensive. But some civil protection pursuant to statute.	Not comprehensive. But some criminal protection pursuant to statute.	No.	Yes.	No.	No.	No.	No.	No.	No.	Yes.	Yes.

GERMANY

Covered Acts

Acts Covered as Civil Infringement		**Acts Covered as Crimes**		**Third Parties:** **Liable for Acquisition?** **Liable Even if Innocent (Without Knowledge)?**	
Breach of Duty?	Wrongful Acquisition/ Misappropriation	Breach of Duty?	Wrongful Acquisition/ Misappropriation	Civil	Criminal
Yes.	Yes.	Yes.	Yes.	Yes. No. Only liable if third party has knowledge or reason to know (“conditional intent”).	Yes. No. Only liable if third party has knowledge or reason to know (“conditional intent”).

Defining Duties and Misappropriation

Defining Duty of Confidentiality			**Restrictions on Duty of confidentiality**		**Defining Wrongful Acquisition - Misappropriation**	
Commercial Relationship	Current Employment Relationship	Past Employment Relationship	Commercial Relationship	Employment Relationship	Civil	Criminal
Duty can be based on express contract or implied. Duty not to disclose for personal gain, competitive purposes, or for benefit of a third party.	Duty can be based on express contract or implied. Duty not to disclose for personal gain, competitive purposes, or for benefit of a third party.	Duty can be based on express agreement or implied, but limited in practice. Implied duty only applies to disclosure to third parties. Employee may use for own benefit rightfully obtained material. Express duty must be specific and cannot amount to a covenant not to compete or impede use of general skills and knowledge. No doctrine of inevitable disclosure.	Regulated strictly under the competition laws. Will be invalid if not limited strictly to the scope of the trade secrets, and contain no extraneous limitations. Ends with public disclosure of confidential information.	Ends with public disclosure of confidential information.	Same as criminal.	Intentional procurement: (a) acquisition through "the use of technical means, such as photocopying, copying of data files, the use of recording or listening devices in cases of oral reproduction of the secrets;"[76] (b) "manufacture of a reproduction of the trade secret, such as the manufacture of a certain recipe or a machine which embodies the secret."[77] (c) "the removal of a thing which embodies the secret. This may be the removal of data carriers, machines or machine elements. The substance or carrier of the embodiment are irrelevant"[78] "Saving" makes it an offense for somebody who already has knowledge (e.g., a departing or departed employee) to download records or make photocopies to preserve or embody their knowledge.

GERMANY

Restrictions on Liability

76 Ibid.

77 Ibid.

78 Mary-Rose McGuire et al., Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, Germany 7 - 8 (2010).

Additional Elements of Proof in Infringement Claim		**Contractual Restrictions on Competition - Validity**		**Defences**	
Civil	Criminal	Commercial Relationship	Post-Employment	Civil	Criminal
None.	None.	Regulated strictly under the competition laws. Will be invalid if not limited strictly to the scope of the trade secrets, and contain no extraneous limitations. Essentially, they must amount to a specific duty not to disclose or use particular trade secrets rather than a duty not to compete.	Doubtful validity. Extensive restrictions: it must be in writing, it must pay 50% of the most recent salary earned during employment (which is often subject to dispute), it must serve a legitimate business interest of the employer, it must be reasonable with respect to geographic scope and duration, and cannot, in any event, last longer than two years.	Independent creation. Reverse engineering.	Independent creation. Reverse engineering.

GERMANY

Remedies

Civil Remedies								**Criminal Remedies**		
Preliminary injunction	Permanent injunction	Injunction to eliminate wrongful head start	Delivery up and/or destruction of infringing materials	Compensatory Damages – Availability and Type	Defendant's Profits	Punitive damages available?	Statutory or Pre-established damages	Fines	Jail Sentence	Other
Yes.	Yes. For so long as remains secret; if defendant acted maliciously, may be barred forever.	No.	Yes.	Direct. Lost Profits. Defendant's profits. Reasonable royalty.	Yes.	No.	No.	5 Euros to 1.8 million Euros.	Two to three years with a maximum of five years in certain cases.	None.

GERMANY

Enforcement, investigation and discovery & related regulations

Enforcement, investigation and discovery			**Data Exclusivity**		**Technology Transfer**	**Legal Complements**
Emergency Search to preserve and obtain proof	Pre-trial discovery	Protection of confidentiality of trade secrets in litigation	Drugs	Agricultural Chemicals		Fraser Score
Available, but high burden makes impracticable. Conducted by an expert.	Unavailable.	In camera hearings available. Protection of documents available. Limited protection from other party available.	"8 + 2 + 1 year approach." Pharmaceutical test data submitted to government for new medicinal products and new indications or uses is protected from disclosure or use for 8 years. Once the 8 year period ends, the data can be used by generic manufacturers to prepare and apply for regulatory approval, but not market a product. This period of market exclusivity lasts 2 years. The initial applicant may receive another 1 year for new indications.	"8 + 2 + 1 year approach." Test data submitted to government for new products and new indications or uses is protected from disclosure or use for 8 years. Once the 8 year period ends, the data can be used by generic manufacturers to prepare and apply for regulatory approval, but not market a product. This period of market exclusivity lasts 2 years. The initial applicant may receive another 1 year for new indications.	None.	On the Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, Germany receives a score of 8.17 out of 10, which ranks it 14th in the world.[79]

[79] Fraser Institute, Economic Freedom of the World 2010 Annual Report at 70 (2010).

GERMANY

Additional Comments

Expert characterisation of the operation of the protection of trade secrets in practice
The specific pleading requirements in civil cases are noted as problematic, impairing the effectiveness of civil remedies: In German law, it is also problematic that in cases where claims are asserted on the basis of a trade secret the secret information must be identified and its content must be described. This involves the risk that the trade secret finally becomes common property or becomes known to the opposing party in more detail. Hence, protection of know-how in (infringement) proceedings has to be assessed as insufficient.[80] Criminal enforcement is relied on heavily in Germany due to limitations in civil cases. However, one expert report observes that "cases that end with a conviction of a perpetrator in a trade secrets case are rare. If there is a conviction, it would usually be a monetary fine."[81] An expert report observed that an employee's lack of duty beyond employment is problematic: "it would be desirable that protection be extended beyond the termination of the employment – for a limited period of time. Such an extension of protection is required at least for the case where the future career of the employee is not affected."[82] An expert reported discussed the desirability of a "head start" injunctions: If a trade secret has been stolen by an unlawful or even criminal violation of secrecy or by industrial espionage by employees or third parties and becomes generally known for that reason, the holder suffers not only damage by the fact that a competitor is now aware of his trade secret. He loses his trade secret as a whole, because it has become common knowledge and is left unprotected against other competitors by this violation. It thus would be desirable if the aggrieved holder, who lost his trade secret without fault, is afforded protection against unfair exploitation at least for a particular transitional period despite the fact that his trade secret has become common knowledge. In another context, both German and European law contain a comparable regulation. Sect. 6 sentence 3 GeschmMG (German Design Act) provides that the disclosure of a design is not detrimental to novelty if such design was disclosed as a consequence of an abusive act against the designer. This legal concept should also be applied to know-how, to ensure that the holder is not affected twice by a punishable act against his trade secret.[83]

SOURCES:
See Annex 2 of this paper for a detailed overview of German trade secret law and sources.

80 Mary-Rose McGuire, et al., Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, Germany 17-18 (2010).

81 Hogan Lovells Report, Appendix 2 at 93.

82 Mary-Rose McGuire, et al., Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, Germany 17 (2010).

83 Ibid.

INDIA

Source of Law, Definition and Scope

Statutory or Other Protection		**Definition**			**Additional Elements of Definition**					**Scope**	
Civil	Criminal	All confidential business information	Common Definition: Confidential business information, **subject to:** deriving value from secrecy; reasonable and making reasonable efforts to maintain secrecy	Common definition **plus condition that** it be imparted to recipient in confidence	Use must be shown	Inventory of trade secrets required	Must be reduced to writing	Must be identified as a trade secret to recipient	Written notice to recipient required	Confidential Business Information	Technical Information
No statutory protection. Civil protection by means of common law, but limited case law and use. May follow English law for guidance.	No.	No.	No.	Yes.	No.	No.	No.	No.	No.	Yes.	Yes.

INDIA

Covered Acts

Acts Covered as Civil Infringement		**Acts Covered as Crimes**		**Third Parties:** **Liable for Acquisition?** **Liable Even if Innocent (Without Knowledge)?**	
Breach of Duty?	Wrongful Acquisition/ Misappropriation	Breach of Duty?	Wrongful Acquisition/ Misappropriation	Civil	Criminal
Use in Breach of Duty. Disclosure in Breach of Duty.	No. India appears to maintain the relationship-based view of trade secret infringement. Courts will thus look to a breach of duty, rather than misappropriation (or breach of a broadly implied duty) via surveillance or trespass.	No.	No.	Yes. No. Knowledge required, or at least reason to know.	Not applicable.

INDIA

Defining Duties and Misappropriation

Defining Duty of Confidentiality			**Restrictions on Duty of confidentiality**		**Defining Wrongful Acquisition - Misappropriation**	
Commercial Relationship	Current Employment Relationship	Past Employment Relationship	Commercial Relationship	Employment Relationship	Civil	Criminal
Duty can be based on express agreement in commercial contract. Duty can be implied in the context of a business relationship – must be imparted under confidential circumstances.	Duty can be based on express agreement only. Duty can be implied in the context of an employment relationship – must be imparted under confidential circumstances.	Duty can be based on express contract. Implied duty can continue after employment terminates. No inevitable disclosure doctrine.	Generally valid.	Generally valid, but neither express nor implied post-employment duties to keep information confidential may cover general skills and knowledge.	Not applicable.	Not applicable.

INDIA

Restrictions on Liability

Additional Elements of Proof in Infringement Claim		**Contractual Restrictions on Competition - Validity**		**Defences**	
Civil	Criminal	Commercial Relationship	Post-Employment	Civil	Criminal
None.	Not applicable.	During the term of a contractual relationship, such agreements are valid, subject to competition law regulation. Post-termination, commercial agreements not to compete generally not enforceable unless the sale of a business in involved. Agreements in restraint of trade are void pursuant to Section 27 of the Contract Act. However, an exception is made in the case of the sale of a business.	Generally not valid.	Independent creation. Reverse engineering.	Not applicable.

INDIA

Remedies

Civil Remedies								**Criminal Remedies**		
Preliminary injunction	Permanent injunction	Injunction to eliminate wrongful head start	Delivery up and/or destruction of infringing materials	Compensatory Damages – Availability and Type	Defendant's Profits	Punitive damages available?	Statutory or Pre-established damages	Fines	Jail Sentence	Other
Yes. Ex parte available.	Yes. (For so long as remains secret)	Yes.	Yes.	Out of pocket. Lost Profits. Consequential. Defendant's profits.	Yes.	No.	No.	None.	None.	None.

INDIA

Enforcement, investigation and discovery & related regulations

Enforcement, investigation and discovery			**Data Exclusivity**		**Technology Transfer**	**Legal Complements**
Emergency Search to preserve and obtain proof	Pre-trial discovery	Protection of confidentiality of trade secrets in litigation	Drugs	Agricultural Chemicals		Fraser Score
Yes. "Anton Piller" Order Ex parte available. A commissioner conducts search.	Documentary and interrogatories under supervision of court.	In camera hearings available. Sealed record available. Protection from other party available.	No data exclusivity.	New products for 3 years. Begins on the date of registration.	Yes. Inbound technology agreements are regulated, but less than in the past. Registration and some substantive review required, unless certain requirements for automatic approval met.	On the Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, India receives a score of 5.93 out of 10, which ranks it 61st in the world.[84] It scores particularly low on legal enforcement of contracts (2.59 out of 10).

84 Fraser Institute, Economic Freedom of the World 2010 Annual Report at 81 (2010).

INDIA

Additional Comments

Expert characterisation of the operation of the protection of trade secrets in practice
• Although trade secret protection is almost exclusively pursuant to the common law, "there is a paucity of case law on the subject of trade secrets,"[85] • "Trade Secrets seems to be a neglected field in India, as there is no enactment or policy framework for the protection of trade secrets."[86] • As of November 2012, there was a report that the Indian government was considering trade secret legislation.[87] • Damages are apparently hard to obtain, a least in contested cases: "The courts have awarded damages but primarily in ex parte case where the defendants have chosen not to contest or even participate. In the cases which are contested, the courts have insisted upon to prove the damages suffered to quantify the claimed damage or avoid such damages. … there are hardly any cases in India post trial where damages have been quantified or awarded or the order of delivery up have been passed. Most of the cases are concluded either ex parte or by way of settlement arrived at between the parties."[88] An AIPPI Report made the following recommendations: [89] (1) Legislation: "It may be further desirable confidential information or trade secrets may also be dealt with by the respective intellectual property legislations such as the ones relating to Trade Marks, Copyright, Industrial Design and Patents so that they may be considered as allied rights protected in the same manner as in other intellectual property." "It is also desirable that the definition of Article 39.2 of TRIPS should be incorporated in the respective legislations since it is comprehensive and addresses relevant factors." (2) Statutory Damages: "Quite often, it may be difficult to prove actual damage and it may be desirable to incorporate the concept of "statutory damage" in cases of breach of all kinds of intellectual property rights including trade secrets and breach of confidence." (3) Summary Adjudication: "Considering the commercial significance and the urgency of adjudication of such matters, it may also be advisable to have a summary procedure for adjudication of such cases. Though the Supreme Court of India has taken a stand in several cases recently that all intellectual property cases should be tried and concluded within four months, the said mandate remains more on paper than in practice."

SOURCES: MacLaren, Trade Secrets Throughout the Work § 19 (2012). Hemant Singh, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, India 6 (2010).

85 MacLaren, Trade Secrets Throughout the Work § 19:2 (2012).

86 Ramesh K. Vaidyanathan, Trade Secrets and Confidential Information, Advaya Legal Law Firm Website (September 2010), http://www.advayalegal.com/trade-secrets-confidential-information.html.

87 Subodh Ghildiyal, Govt working on norms to protect trade secrets, The Times of India (29 November 2012), http://timesofindia.indiatimes.com/business/india-business/Govt-working-on-norms-to-protect-trade-secrets/articleshow/17409936.cms.

88 Hemant Singh, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, India 6 (2010).

89 Hemant Singh, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, India 10 (2010).

ISRAEL

Source of Law, Definition and Scope

Statutory or Other Protection		**Definition**			**Additional Elements of Definition**					**Scope**	
Civil	Criminal	All confidential business information	Common Definition: Confidential business information, **subject to:** deriving value from secrecy; reasonable and making reasonable efforts to maintain secrecy	Common definition **plus condition that** it be imparted to recipient in confidence	Use must be shown	Inventory of trade secrets required	Must be reduced to writing	Must be identified as a trade secret to recipient	Written notice to recipient required	Confidential Business Information	Technical Information
Comprehensive civil protection pursuant to the Commercial Torts Law of 1999.	No. (Except for statute related to state security).	No.	Yes.	No.	No.	No.	No.	No.	No.	Yes.	Yes.

ISRAEL

Covered Acts

Acts Covered as Civil Infringement		**Acts Covered as Crimes**		**Third Parties:** **Liable for Acquisition?** **Liable Even if Innocent (Without Knowledge)?**	
Breach of Duty?	Wrongful Acquisition / Misappropriation	Breach of Duty?	Wrongful Acquisition / Misappropriation	Civil	Criminal
Use in Breach of Duty. Disclosure in Breach of Duty.	Yes. Very broad. See definition below.	Not applicable.	Not applicable. Note that Penal Law of 1977 protects a limited category of confidential information—information related to state security—which includes a wide variety of confidential information, including trade secrets that are owned by either the state or an individual and held by the state.[90]	Yes. No. Only liable if third party has knowledge or reason to know. Innocent third party exempt if received in good faith and for consideration.	Not applicable.

[90] Section 91 of the Penal Law.

ISRAEL

Defining Duties and Misappropriation

Defining Duty of Confidentiality			**Restrictions on Duty of confidentiality**		**Defining Wrongful Acquisition - Misappropriation**	
Commercial Relationship	Current Employment Relationship	Past Employment Relationship	Commercial Relationship	Employment Relationship	Civil	Criminal
Duty can be based on express agreement in commercial contract. Duty can be implied in the context of a business relationship.	Duty can be based on express agreement and implied duty.	Duty can be based on express contract. Duty is also implied. No inevitable disclosure doctrine.	None.	Express and implied post-employment duties to keep information confidential likely unenforceable with respect to general skills and knowledge.	The mere taking of a trade secret will give rise to a cause of action.”[91] Israel’s law takes a unique route to determining fault in trade secret cases. Section 10 of the Commercial Torts Act, in essence, “adopts the copyright presumption of ‘similarity + access = infringement.’”[92]	Not applicable.

91 Tal Band & Ilan Miller, Question Q215: Protection of Trade Secrets Through IPR and Unfair Competition Law, AIPPI Report on Israel, 5 (2010). https://www.aippi.org/download/commitees/215/GR215israel.pdf

92 Ibid.

ISRAEL

Restrictions on Liability

Additional Elements of Proof in Infringement Claim		**Contractual Restrictions on Competition - Validity**		**Defences**	
Civil	Criminal	Commercial Relationship	Post-Employment	Civil	Criminal
None.	Not applicable.	Commercial agreements not to compete generally enforceable, subject to a two-part test: (1) the restrictions must be no broader than reasonably necessary to protect the legitimate interests of the parties; and (2) the restrictions should not harm the public. Reasonableness of a non-competition clause is a function of the length and geographic breadth of the clause.[93]	Two-part test is applicable. Courts reluctant to enforce if negatively affect ability to earn a living. Post-employment agreements not to compete enforceable if reasonable with respect to competitive need, time and geographic scope.	Independent creation. Reverse engineering.	Not applicable.

[93] MacLaren, Trade Secrets Throughout the World, Section 21.8 (2012).

ISRAEL

Remedies

Civil Remedies								**Criminal Remedies**		
Preliminary injunction	Permanent injunction	Injunction to eliminate wrongful head start	Delivery up and/or destruction of infringing materials	Compensatory Damages – Availability and Type	Defendant's Profits	Punitive damages available?	Statutory or Pre-established damages	Fines	Jail Sentence	Other
Yes.	Yes. (For so long as remains secret).	Uncertain.	Yes.	Out of pocket. Lost Profits. Consequential. Defendant's profits.	Yes.	No.	Yes. Up to NIS 100 000 per tortious act regardless of actual damages.	Not applicable.	Not applicable.	Not applicable.

ISRAEL

Enforcement, investigation and discovery & related regulations

Enforcement, investigation and discovery			**Data Exclusivity**		**Technology Transfer**	**Legal Complements**
Emergency Search to preserve and obtain proof	Pre-trial discovery	Protection of confidentiality of trade secrets in litigation	Drugs	Agricultural Chemicals	Civil	Fraser Score
Yes. A court appointed "temporary receiver," not plaintiff, may conduct search. Ex parte available.	Documentary. Interrogatories. At initiative of party.	Full protection with respect to hearings (in camera hearings available). Protection from other party available, but pursuant to a protective order, not limited access.	New active ingredients only. "6.5 years, calculated from the first product registration of the pharmaceutical in a number of developed reference countries including the United States and the European Union."[94] Data is subject to exclusivity, not protection. Generics can file based on bioequivalence before end of period, but not market until end of period.	10 years, apparently. (Based on tentative information reported by the authorities. Subject to confirmation via published sources, pending.)	None.	On the Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, Israel receives a score of 5.90 out of 10, which ranks it 62nd in the world. It receives middling scores on most sub-components, but receives a relatively low score with respect to enforcement of contract (3.46 out of 10) and a relatively high score with respect to judicial independence (8.38 out of 10).

94 Trade Policy Review Body – Report by the Secretariat – Israel, WT/TPR/S/272, 52 (25 September 2012).

ISRAEL

Additional Comments

Expert characterisation of the operation of the protection of trade secrets in practice
Commentators have described Israel's civil protection of trade secrets as broad and affording adequate protection to trade secret owners,[95] with the courts granting a broad definition with a wide and varied subject matter.[96] Israel does not have comprehensive criminal protection.

SOURCES:

See Annex 2 of this paper for a detailed overview of Israel's trade secret law and sources.

ITALY

Source of Law, Definition and Scope

95 Tal Band & Ilan Miller, Question Q215: Protection of Trade Secrets Through IPR and Unfair Competition Law, AIPPI Report on Israel, 9 (2010). https://www.aippi.org/download/commitees/215/GR215israel.pdf

96 MacLaren, Trade Secrets Throughout the World, Section 21.4 (2012).

Statutory or Other Protection		**Definition**			**Additional Elements of Definition**					**Scope**	
Civil	Criminal	All confidential business information	Common Definition: Confidential business information, **subject to:** deriving value from secrecy; reasonable and making reasonable efforts to maintain secrecy	Common definition **plus condition that** it be imparted to recipient in confidence	Use must be shown	Inventory of trade secrets required	Must be reduced to writing	Must be identified as a trade secret to recipient	Written notice to recipient required	Confidential Business Information	Technical Information
Yes.	No comprehensive law, but there are limited statutes applying to employees and unauthorized use of documents and other media.	No.	Yes. Italy adopted Articles 39(2) and 39(3) of TRIPS verbatim.	No.	No.	No.	No.	No.	No.	Yes.	Yes.

ITALY

Covered Acts

Acts Covered as Civil Infringement		**Acts Covered as Crimes**		**Third Parties:** **Liable for Acquisition?** **Liable Even if Innocent (Without Knowledge)?**	
Breach of Duty?	Wrongful Acquisition/ Misappropriation	Breach of Duty?	Wrongful Acquisition/ Misappropriation	Civil	Criminal
Yes, but trade secret protection is broader, since trade secrets are treated as IP rights.	Yes. Very broad. See definition below.	Yes. An employee is liable for unauthorized use or disclosure of an employer's secret obtained in the course of employment.	Not applicable; third parties are not liable under criminal law.	Yes. No. Only liable if third party has knowledge or reason to know. Innocent third party exempt if received in good faith and for consideration.	No.

ITALY

Defining Duties and Misappropriation

Defining Duty of Confidentiality			**Restrictions on Duty of confidentiality**		**Defining Wrongful Acquisition - Misappropriation**	
Commercial Relationship	Current Employment Relationship	Past Employment Relationship	Commercial Relationship	Employment Relationship	Civil	Criminal
Trade secrets are treated as IP rights; third parties must only use them within the scope of permission. Thus, duties are very broad.	Trade secrets are treated as IP rights; third parties must only use them within the scope of permission. Thus, duties are very broad.	Trade secrets are treated as IP rights; third parties must only use them within the scope of permission. Thus, duties are very broad. Specifically, express contracts remain in force.	None.	None.	The mere taking of a trade secret constitutes misappropriation, as the offense includes acquiring, using, or disclosing the information without the owner's consent.	Not applicable.

ITALY

Restrictions on Liability

Additional Elements of Proof in Infringement Claim		**Contractual Restrictions on Competition - Validity**		**Defences**	
Civil	Criminal	Commercial Relationship	Post-Employment	Civil	Criminal
None.	None.	Commercial agreements not to compete generally enforceable, subject to competition regulations.	Non-competition clauses are not enforceable unless they meet the following requirements: (1) they must be limited in time—5 years for executives and 3 years for other employees; (2) they must be limited in geographic scope; (3) they must cover specific work activities; and (4) they must pay compensation no lower than 20 – 30% of monthly salary, including benefits and bonuses.[97]	Independent creation.	Not applicable.

[97] Ibid. at 53.

ITALY

Remedies

Civil Remedies								Criminal Remedies		
Preliminary injunction	Permanent injunction	Injunction to eliminate wrongful head start	Delivery up and/or destruction of infringing materials	Compensatory Damages – Availability and Type	Defendant's Profits	Punitive damages available?	Statutory or Pre-established damages	Fines	Jail Sentence	Other
Yes.	Yes.	Uncertain.	Yes.	Out of pocket. Lost Profits. Consequential	Yes.	No.	No.	Penalties of up to 516 Euros for use or disclosure of a secret obtained during the course of employment.[98]	Penalties of up to 1 year in jail for use or disclosure of a secret obtained during the course of employment.[99] Penalties of up to 2 years in jail for use or disclosure of a secret regarding scientific discoveries, inventions, or industrial applications learned during the course of employment.[100]	None.

98 Article 622 of the Italian Criminal Code.

99 Article 622 of the Italian Criminal Code.

100 Article 623 of the Italian Criminal Code.

ITALY

Enforcement, investigation and discovery & related regulations

Enforcement, investigation and discovery			**Data Exclusivity**		**Technology Transfer**	**Legal Complements**
Emergency Search to preserve and obtain proof	Pre-trial discovery	Protection of confidentiality of trade secrets in litigation	Drugs	Agricultural Chemicals		Fraser Score
Yes. Plaintiff may conduct search accompanied by bailiff and expert. Ex parte available.	Limited discovery of documents under supervision of court.	Partial protection with respect to hearings -investigative hearings are non-public, but final hearings before the Judges issuing a decision are public. No protection from other party. Final decision must be public.	"8 + 2 + 1 year approach." Pharmaceutical test data submitted to government for new medicinal products and new indications or uses is protected from disclosure or use for 8 years. Once the 8 year period ends, the data can be used by generic manufacturers to prepare and apply for regulatory approval, but not market a product. This period of market exclusivity lasts 2 years. The initial applicant may receive another 1 year for new indications.	"8 + 2 + 1 year approach." Test data submitted to government for new products and new indications or uses is protected from disclosure or use for 8 years. Once the 8 year period ends, the data can be used by generic manufacturers to prepare and apply for regulatory approval, but not market a product. This period of market exclusivity lasts 2 years. The initial applicant may receive another 1 year for new indications.	None.	On the Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, Italy receives a score of 5.67 out of 10, which ranks it 55th in the world. It ranks relatively low with respect to judicial independence (3.56 out of 10), impartial courts (2.60 out of 10), and legal enforcement of contract (3.18 out of 10).

ITALY

Additional Comments

Expert characterisation of the operation of the protection of trade secrets in practice
A recent commentator noted the recent vintage of trade secret law as a challenge: > Notwithstanding the fact that our country has implemented the TRIPs agreement and the EC Enforcement Directive, since the provisions recognizing the protection of trade secrets as an IP right have been introduced in our IP Code only recently, there is not yet a reliable case law allowing a stable interpretation of the rules.[101] While Italy has criminal protection against trade secret theft, its scope is limited to employees. Therefore, most claims are brought as civil claims: "Most claims for trade secret infringement are brought under Articles 98 and 99 IPC, given the broader scope of protection granted by those provisions and the wide array of available civil remedies."[102]

SOURCES:

See Annex 2 of this paper for a detailed overview of Italy's trade secret law and sources.

101 Lamberto Liuzzo et al., Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, Italy, 11 (2010).

102 Hogan Lovells Report, Appendix 2, at 158 (2012).

JAPAN

Source of Law, Definition and Scope

Statutory or Other Protection		**Definition**			**Additional Elements of Definition**					**Scope**	
Civil	Criminal	All confidential business information	Common Definition: Confidential business information, **subject to:** deriving value from secrecy; reasonable and making reasonable efforts to maintain secrecy	Common definition **plus condition that** it be imparted to recipient in confidence	Use must be shown	Inventory of trade secrets required	Must be reduced to writing	Must be identified as a trade secret to recipient	Written notice to recipient required	Confidential Business Information	Technical Informatio n
Yes. Comprehensive statutory protection pursuant to the Unfair Competition Prevention Act.	Yes. Comprehensive statutory protection pursuant to the Unfair Competition Prevention Act.	No.	Yes.	No.	No.	No.	No.	No.	No.	Yes.	Yes.

JAPAN

Covered Acts

Acts Covered as Civil Infringement		**Acts Covered as Crimes**		**Third Parties:** **Liable for Acquisition?** **Liable Even if Innocent (Without Knowledge)?**	
Breach of Duty?	Wrongful Acquisition/ Misappropriation	Breach of Duty?	Wrongful Acquisition/ Misappropriation	Civil	Criminal
Use in Breach of Duty. Disclosure in Breach of Duty.	Yes. Wrongful acquisition is broadly understood as both wrongful acts and commercial espionage.	Yes.	Yes.	Yes. No. Knowledge required, or at least reason to know (gross negligence). However, liable once knowledge is acquired.	Yes. No. Knowledge required, or at least reason to know (gross negligence). However, liable once knowledge is acquired.

JAPAN

Defining Duties and Misappropriation

Defining Duty of Confidentiality			**Restrictions on Duty of confidentiality**		**Defining Wrongful Acquisition - Misappropriation**	
Commercial Relationship	Current Employment Relationship	Past Employment Relationship	Commercial Relationship	Employment Relationship	Civil	Criminal
Duty can be based on express agreement in commercial contract. Duty can be implied in the context of a business relationship.	Duty can be based on express agreement. Duty can be implied in the context of an employment relationship.	Duty can be based on express contract. Implied duty can continue after employment terminates. No inevitable disclosure doctrine.	Generally valid.	Generally valid, but neither express nor implied post-employment duties to keep information confidential may cover general skills and knowledge.	"Acts of acquiring a trade secret by theft, fraud, duress or other wrongful means."	"Acts of acquiring a trade secret by theft, fraud, duress or other wrongful means."

JAPAN

Restrictions on Liability

Additional Elements of Proof in Infringement Claim		**Contractual Restrictions on Competition - Validity**		**Defences**	
Civil	Criminal	Commercial Relationship	Post-Employment	Civil	Criminal
None.	None.	During the term of a contractual relationship, such agreements are valid, subject to competition law regulation. Post-termination, commercial agreements not to compete generally enforceable subject to reasonable limits on duration and geography.	During the term of an employment relationship, such agreements are valid, subject to competition law regulation. Post-termination, agreements not to compete generally enforceable subject to reasonable limits on duration and geography.	Independent creation. Reverse engineering.	Independent creation. Reverse engineering.

JAPAN

Remedies

Civil Remedies								**Criminal Remedies**		
Preliminary injunction	Permanent injunction	Injunction to eliminate wrongful head start	Delivery up and/or destruction of infringing materials	Compensatory Damages – Availability and Type	Defendant's Profits	Punitive damages available?	Statutory or Pre-established damages	Fines	Jail Sentence	Other
Yes. Ex parte not available.	Yes. (For so long as remains secret).	Yes.	Yes.	Out of pocket. Lost Profits. Consequential. Defendant's profits. Royalties.	Yes.	No.	No.	Yes. For individuals, a fine of up to ten million yen. For a corporation, up to 300 million yen.	Yes. For individuals, up to 10 years imprisonment.	None.

JAPAN

Enforcement, investigation and discovery & related regulations

Enforcement, investigation and discovery			**Data Exclusivity**		**Technology Transfer**	**Legal Complements**
Emergency Search to preserve and obtain proof	Pre-trial discovery	Protection of confidentiality of trade secrets in litigation	Drugs	Agricultural Chemicals		Fraser Score
Limited. Ex parte not available. No search.	Limited. Effectively very little.	In civil cases: In camera hearings available. Sealed record available. Protection from other party available. In criminal cases: Very little to none.	For new chemical entities, it provides up to 8 years during which data submitted for regulatory approval is protected from disclosure cannot be relied upon by a third party to obtain approval. It provides 4–6 years of protection for certain improvements. Finally, it provides 10 years for orphan drugs.	For new chemical entities, it provides up to 8 years during which data submitted for regulatory approval is protected from disclosure cannot be relied upon by a third party to obtain approval. It provides 4 – 6 years of protection for certain improvements.		On the Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, Japan receives a score of 7.49 out of 10, which ranks it 28th in the world. Its lowest scores are with respect to impartial courts (5.92 out of 10) and legal enforcement of contracts (5.8 out of 10).

JAPAN

Additional Comments

Expert characterisation of the operation of the protection of trade secrets in practice
Japan has comprehensive, strong trade secret protection according to commentators. However there are a few caveats. Injunctions are slow and ex parte ones are not available: "A holder of trade secret may exercise his right to seek injunction through a normal civil trial or the filing of a motion for preliminary injunction. However, in the case of a motion for preliminary injunction, it is legally necessary in principle that there is a court hearing with the presence of the respondent. Although the proceedings for preliminary injunction are faster than a normal civil trial, it usually takes several months before a ruling is made."[103] Trade secrets are poor protected during criminal litigation: "At present, a challenge is how trade secretes should be protected in criminal proceedings in the case of a trial against a crime related to trade secret infringement. It is hoped that a system will be created to protect trade secrets in criminal proceedings, while respecting the constitutional requirements of openness of a trial."[104] The lack of secrecy in criminal litigation discourages use of criminal proceedings: "In reality, however, these criminal remedies are rarely used against the acts of trade secret infringement. One of the main reasons for this is that there is no system in place for preventing the publication of trade secrets to be tried in criminal proceedings, which is related to the fact that the openness of a trial is guaranteed by the Constitution."[105] AIPPI 9

SOURCES:

MacLaren, Trade Secrets Throughout the Work § 23 (2012).
Kazuo Ubukata, Question Q215: Protection of Trade Secrets Through IPR and Unfair Competition Law, AIPPI Report on Japan (2010).

103 Kazuo Ubukata, Question Q215: Protection of Trade Secrets Through IPR and Unfair Competition Law, AIPPI Report on Japan 8 (2010).

104 Ibid at 19.

105 Ibid at 9.

KOREA

Source of Law, Definition and Scope

Statutory or Other Protection		**Definition**			**Additional Elements of Definition**					**Scope**	
Civil	Criminal	All confidential business information	Common Definition: Confidential business information, **subject to:** deriving value from secrecy; reasonable and making reasonable efforts to maintain secrecy	Common definition **plus condition that** it be imparted to recipient in confidence	Use must be shown	Inventory of trade secrets required	Must be reduced to writing	Must be identified as a trade secret to recipient	Written notice to recipient required	Confidential Business Information	Technical Information
Yes. Comprehensive statutory protection.	Yes. Comprehensive statutory protection.	No.	Yes.	No.	No.	No.	No.	No.	No.	Yes.	Yes.

KOREA

Covered Acts

Acts Covered as Civil Infringement		**Acts Covered as Crimes**		**Third Parties:** **Liable for Acquisition?** **Liable Even if Innocent (Without Knowledge)?**	
Breach of Duty?	Wrongful Acquisition/ Misappropriation	Breach of Duty?	Wrongful Acquisition/ Misappropriation	Civil	Criminal
Yes.	Yes.	Yes. (1) Knowingly acquiring, using, or disclosing a trade secret for use in a foreign country, or (2) Knowingly acquiring, using, or disclosing a trade secret for personal gain or to do damage to the owner.	Yes. Knowingly acquiring, using, or disclosing a trade secret for personal gain or to do damage to the owner.	Yes. No. Only liable if third party has knowledge or reason to know (gross negligence). Innocent third party not liable.	No.

KOREA

Defining Duties and Misappropriation

Defining Duty of Confidentiality			**Restrictions on Duty of confidentiality**		**Defining Wrongful Acquisition - Misappropriation**	
Commercial Relationship	Current Employment Relationship	Past Employment Relationship	Commercial Relationship	Employment Relationship	Civil	Criminal
Express agreement gives rise to duty. Can likely be implied in business relationships.	Express agreement gives rise to duty. Can likely be implied in employment relationships.	Express contracts remain in force. There is disagreement as to whether an implied duty continues after the end of employment.[106] Inevitable disclosure may prevent employee from doing particular work for a new employer, but not from taking a job with competitor at all.	None.	Express post-employment confidentiality obligations are enforceable if reasonable, but not with respect to employee's general skills and knowledge.	Includes torts, crimes, but also circumventing owner's attempts to maintain secrecy.	Knowingly acquiring, using, or disclosing a trade secret for personal gain or to do damage to the owner.

106 Hyun-Soo Kim, Trade secret law, intellectual property, and innovation: Theoretical, empirical, and Asian perspectives, PhD Thesis, University of Illinois 139 (2011).

KOREA

Restrictions on Liability

Additional Elements of Proof in Infringement Claim		**Contractual Restrictions on Competition - Validity**		**Defences**	
Civil	Criminal	Commercial Relationship	Post-Employment	Civil	Criminal
None.	None.	Commercial agreements not to compete generally enforceable, subject to competition regulations.	Express post-employment confidentiality obligations are enforceable if reasonable. The factors considered include "the existence of protectable employer interests, a former employee's position in a former employer's firm, durational and geographical scope of the restraint, field of work, the existence of compensation offered to an employee, reasons for termination of the employment relationship, public interests, and so on."[107]	Independent creation.	Independent creation.

[107] Ibid at 145 (translating and quoting Seoul Central District Court of Korea, Decision of 19 March 2008, Case No. 2007kahap3903).

KOREA

Remedies

Civil Remedies								**Criminal Remedies**		
Preliminary injunction	Permanent injunction	Injunction to eliminate wrongful head start	Delivery up and/or destruction of infringing materials	Compensatory Damages – Availability and Type	Defendant's Profits	Punitive damages available?	Statutory or Pre-established damages	Fines	Jail Sentence	Other
Yes.	Yes.	Uncertain.	Yes.	Actual damages. Plaintiff's lost profits. Defendant's profits. Reasonable Royalty.	Yes.	No.	No.	Not less than 2 times but not more than 10 times the proprietary profit amount (applicable to both types of trade secret crimes).	Up to 10 years for knowingly acquiring, disclosing, or using trade secret for use in foreign country. Up to 5 years for acquiring, using or disclosing for personal gain or to do damage to owner.	None.

KOREA

Enforcement, investigation and discovery & related regulations

Enforcement, investigation and discovery			**Data Exclusivity**		**Technology Transfer**	**Legal Complements**
Emergency Search to preserve and obtain proof	Pre-trial discovery	Protection of confidentiality of trade secrets in litigation	Drugs	Agricultural Chemicals		Fraser Score
None.	Limited discovery of documents at pre-trial hearings under supervision of court.	No protection with respect to hearings. Protection (as of 2012) with respect to the record.	Five years of data exclusivity from the date of marketing approval for new pharmaceuticals. Three years of data exclusivity from the date of marketing approval for new clinical information for previously approved chemical entities.	Ten years of data exclusivity for new agricultural chemical products. Ten years of data exclusivity for a new use of previously approved agricultural chemical products.	Although technology licenses were regulated in the past, there are few remaining requirements. The Foreign Investment Protection Law restricts inbound licenses that interfere with national security or public order. It also requires that agreements be reported (but not approved) in the case of licenses that last more than one year and involve (i) aerospace; (ii) defence; or (iii) advanced technology. This is a reporting, not approval, requirement.	On the Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, Korea receives a score of 6.76 out of 10, which ranks it 31st in the world. It ranks relatively low on judicial independence (5.13 out of 10) and impartial courts (4.37 out of 10).

KOREA

Additional Comments

Expert characterisation of the operation of the protection of trade secrets in practice
Commentators observe that Korea has grown increasingly protective of trade secrets, but some parties continue to express specific concerns. As Korea has become a leader in innovation and high technology manufacturer, trade secret protection has been viewed as and treated as increasingly important.[108] However, parties have complained that test data filed to comply with regulatory requirements has leaked to competitors.[109] A 2011 Investment Climate Statement by the US Department of State observed: > Korean laws on unfair competition and trade secrets provide a basic level of trade secret protection in Korea, but are insufficient in some instances. For example, some US firms, particularly certain manufacturers of chemicals, pet food, cosmetics, and food products, face continuing problems with government regulations requiring submission of very detailed product information, such as formula or blueprints, as part of registration or certification procedures. US firms report that, although the release of business confidential information is forbidden under Korean law, in some instances, government officials do not sufficiently protect this proprietary information, and trade secrets appear to have been made available to Korean competitors or to their trade associations.[110]

SOURCES:
See Annex 2 of this paper for a detailed overview of Korea's trade secret law and sources.

108 Ibid. See also Hyun-Soo Kim, Trade secret law, intellectual property, and innovation: Theoretical, empirical, and Asian perspectives, PhD Thesis, University of Illinois (2011); Mirjana Stankovic, Trade Secrets: South Korea versus United States (2010), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1678768.

109 AMCham Korea, Intellectual Property Rights (2004), http://www.amchamkorea.org/publications/2004ikbc/Intellectual%20Property%20Rights.doc.

110 2011 Investment Climate Statement – Republic of Korea, U.S. Department of State (March 2011), http://www.state.gov/e/eb/rls/othr/ics/2011/157359.htm.

MALAYSIA

Source of Law, Definition and Scope

Statutory or Other Protection		**Definition**			**Additional Elements of Definition**					**Scope**	
Civil	Criminal	All confidential business information	Common Definition: Confidential business information, **subject to:** deriving value from secrecy; reasonable and making reasonable efforts to maintain secrecy	Common definition **plus condition that** it be imparted to recipient in confidence	Use must be shown	Inventory of trade secrets required	Must be reduced to writing	Must be identified as a trade secret to recipient	Written notice to recipient required	Confidential Business Information	Technical Information
No statutory protection. Civil protection by means of common law, with reference to English law.	No. (Beyond certain very isolated and specific offenses).	No.	No.	Yes.	No.	No.	No.	No.	No.	Yes.	Yes.

MALAYSIA

Covered Acts

Acts Covered as Civil Infringement		**Acts Covered as Crimes**		**Third Parties:** **Liable for Acquisition?** **Liable Even if Innocent (Without Knowledge)?**	
Breach of Duty?	Wrongful Acquisition/ Misappropriation	Breach of Duty?	Wrongful Acquisition/ Misappropriation	Civil	Criminal
Use in Breach of Duty. Disclosure in Breach of Duty.	No. Malaysia appears to maintain the relationship-based view of trade secret infringement. Courts will thus look to a breach of duty, rather than misappropriation (or breach of a broadly implied duty) via surveillance or trespass.	No.	No.	Yes. No. Knowledge required, or at least reason to know. But will be restrained after notice.	Not applicable.

MALAYSIA

Defining Duties and Misappropriation

Defining Duty of Confidentiality			**Restrictions on Duty of confidentiality**		**Defining Wrongful Acquisition - Misappropriation**	
Commercial Relationship	Current Employment Relationship	Past Employment Relationship	Commercial Relationship	Employment Relationship	Civil	Criminal
Duty can be based on express agreement in commercial contract. Duty can be implied in the context of a business relationship.	Duty can be based on express agreement. Duty can be implied in the context of an employment relationship. Broad during employment relationship, but limited specifically to trade secrets afterward.	Duty can be based on express contract. Implied duty can continue after employment terminates. No inevitable disclosure doctrine.	Generally valid.	Generally valid, but neither express nor implied post-employment duties to keep information confidential may cover general skills and knowledge	Not applicable.	Not applicable.

MALAYSIA

Restrictions on Liability

Additional Elements of Proof in Infringement Claim		**Contractual Restrictions on Competition - Validity**		**Defences**	
Civil	Criminal	Commercial Relationship	Post-Employment	Civil	Criminal
Detriment must be shown.	Not applicable.	Void pursuant to Section 28 of the Contracts Act, except: - In the case of the sale of a business, within specified reasonable geographic limits. - Upon dissolution of a partnership.	Void pursuant to Section 28 of the Contracts Act.	Independent creation. Reverse engineering.	Not applicable.

MALAYSIA

Remedies

Civil Remedies								**Criminal Remedies**		
Preliminary injunction	Permanent injunction	Injunction to eliminate wrongful head start	Delivery up and/or destruction of infringing materials	Compensatory Damages – Availability and Type	Defendant's Profits	Punitive damages available?	Statutory or Pre-established damages	Fines	Jail Sentence	Other
Yes. Ex parte available.	Yes. (For so long as remains secret).	Yes.	Yes.	Out of pocket. Lost Profits. Consequential. Defendant's profits.	Yes.	No.	No.	None.	None.	None.

MALAYSIA

Enforcement, investigation and discovery & related regulations

Enforcement, investigation and discovery			**Data Exclusivity**		**Technology Transfer**	**Legal Complements**
Emergency Search to preserve and obtain proof	Pre-trial discovery	Protection of confidentiality of trade secrets in litigation	Drugs	Agricultural Chemicals		Fraser Score
Yes. "Anton Piller" Orders are available. Ex parte available. Plaintiff's lawyers conduct search. Often prompts settlement.	Documentary under supervision of court.	Protective orders to prevent disclosure of documents available. In camera proceedings available.	Five years for new drug; three years for a new indication (effective March 2011).	Uncertain.	None.	On the Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, Malaysia receives a score of 6.24 out of 10, which ranks it 49th in the world.[111] It scores particularly low on legal enforcement of contracts (4.38 out of 10).

111 Fraser Institute, Economic Freedom of the World 2010 Annual Report at 102 (2010).

MALAYSIA

Additional Comments

Expert characterisation of the operation of the protection of trade secrets in practice
Publically available commentary on trade secret law in Malaysia is sparse. One commentator observes that "the applicable case law is not well developed. However, the broad principles established in the English cases and in particular *Coco v. Clark* may be equally applicable in Malaysia."[112]

SOURCES:

MacLaren, Trade Secrets Throughout the World § 25:7 (2012).

112 MacLaren, Trade Secrets Throughout the World § 25:7 (2012).

NEW ZEALAND

Source of Law, Definition and Scope

Statutory or Other Protection		**Definition**			**Additional Elements of Definition**					**Scope**	
Civil	Criminal	All confidential business information	Common Definition: Confidential business information, **subject to:** deriving value from secrecy; reasonable and making reasonable efforts to maintain secrecy	Common definition **plus condition that** it be imparted to recipient in confidence	Use must be shown	Inventory of trade secrets required	Must be reduced to writing	Must be identified as a trade secret to recipient	Written notice to recipient required	Confidential Business Information	Technical Information
Comprehen-sive civil protection by means of common law.	Yes. Section 230(2) of the Crimes Act 1961.	No.	No.	Yes.	No.	No.	No.	No.	No.	Yes.	Yes.

NEW ZEALAND

Covered Acts

Acts Covered as Civil Infringement		**Acts Covered as Crimes**		**Third Parties:** **Liable for Acquisition?** **Liable Even if Innocent (Without Knowledge)?**	
Breach of Duty?	Wrongful Acquisition/ Misappropriation	Breach of Duty?	Wrongful Acquisition/ Misappropriation	Civil	Criminal
Use in Breach of Duty. Disclosure in Breach of Duty.	No. New Zealand appears to maintain the relationship-based view of trade secret infringement. Courts will thus look to a breach of duty, rather than misappropriation (or breach of a broadly implied duty) via surveillance or trespass.	No.	Yes. But limited to misappropriating (by taking, obtaining, or copying) a physical document, model or depiction.	Yes. No. Knowledge required, or at least reason to know.	Yes. No. Requires misappropriation (by taking, obtaining, or copying) of a physical document, model or depiction of a trade secret with knowledge that it contains a trade secret.

NEW ZEALAND

Defining Duties and Misappropriation

Defining Duty of Confidentiality			**Restrictions on Duty of confidentiality**		**Defining Wrongful Acquisition - Misappropriation**	
Commercial Relationship	Current Employment Relationship	Past Employment Relationship	Commercial Relationship	Employment Relationship	Civil	Criminal
Duty can be based on express agreement in commercial contract. Duty can be implied in the context of a business relationship.	Duty can be based on express agreement and implied duty. Implied duty broad during employment – covers information beyond strict trade secret definition.	Duty can be based on express contract. Duty is also implied. Implied duty narrower after employment – only trade secrets. No inevitable disclosure doctrine.	None.	Express agreements may cover general skills and knowledge. Implied post-employment duties to keep information confidential likely unenforceable with respect to general skills and knowledge.	No.	Taking, obtaining, or copying without claim of right a physical document, model or depiction of trade secret. Under Section 230(1) of the Crimes Act 1961, culpability is based on the "intent to obtain any pecuniary advantage or to cause loss to any other person."

NEW ZEALAND

Restrictions on Liability

Additional Elements of Proof in Infringement Claim		**Contractual Restrictions on Competition - Validity**		**Defences**	
Civil	Criminal	Commercial Relationship	Post-Employment	Civil	Criminal
Detriment must be shown.	None.	Commercial agreements not to compete generally enforceable.	Courts reluctant to enforce if negatively affect ability to earn a living. Post-employment agreements not to compete enforceable if reasonable with respect to competitive need, time and geographic scope.	Independent creation. Reverse engineering.	No express statutory defences and there appears to be no case law interpreting them. Since the definition excludes "claim of right" and covers only taking trade secrets, independent creation and reverse engineering are likely defences.

NEW ZEALAND

Remedies

Civil Remedies								**Criminal Remedies**		
Preliminary injunction	Permanent injunction	Injunction to eliminate wrongful head start	Delivery up and/or destruction of infringing materials	Compensatory Damages – Availability and Type	Defendant's Profits	Punitive damages available?	Statutory or Pre-established damages	Fines	Jail Sentence	Other
Yes.	Yes. (For so long as remains secret).	Yes, even where information has since become public.	Yes.	Out of pocket. Lost Profits. Consequential. Defendant's profits.	Yes.	Yes.	No.	None.	5 years imprisonment.	None.

NEW ZEALAND

Enforcement, investigation and discovery & related regulations

Enforcement, investigation and discovery			**Data Exclusivity**		**Technology Transfer**	**Legal Complements**
Emergency Search to preserve and obtain proof	Pre-trial discovery	Protection of confidentiality of trade secrets in litigation	Drugs	Agricultural Chemicals	Civil	Fraser Score
Yes. "Anton Piller" Order. Ex parte available. Plaintiff may conduct search. Level of proof greater than for preliminary injunction.	Documentary. At initiative of party.	Full protection with respect to hearings (in camera hearings available). Protection from other party available (protective orders, measures limiting viewing to counsel or other professionals).	New chemical entities only. 5 years.[113] Begins on the date of registration. No other party may receive the registrant's data nor may they rely on it for an application to register an equivalent product. There is no data exclusivity period for data relating to new uses or formulations of old active ingredients.	New chemical entities only. 5 years. Begins on the date of registration. No other party may receive the registrant's data nor may they rely on it for an application to register an equivalent product. There is no data exclusivity period for data relating to new uses or formulations of old active ingredients.	None.	On the Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, New Zealand receives a score of 9.03 out of 10, which ranks it 6th in the world.

113 In correspondence with the OECD Secretariat (October 2013), the New Zealand authorities note that a further three years of protection will be provided in cases of new uses of known compounds.

NEW ZEALAND

Additional Comments

Expert characterisation of the operation of the protection of trade secrets in practice
Criticism of New Zealand's trade secret law is minimal. However, one commentator noted that it is not as developed as in some jurisdictions: By comparison with other larger common law jurisdictions, there has been limited case law on trade secrets and confidential information in New Zealand. Fact situations that have given rise to finer legal issues in other jurisdictions have not, as yet, been litigated in New Zealand. This means that some of the finer points of law have yet to be decided by a New Zealand court. MacLaren Trade Secrets Throughout the World § 29:1 (2012). Of course, as a common law country, New Zealand courts have resort to the decisions of other jurisdictions for guidance, particularly England, Australia, and Canada. Two authorities note that there appears to be no case law concerning the criminal statute, Section 230.[114]

SOURCES:
See Annex 2 of this paper for a detailed overview of New Zealand's trade secret law and sources.

[114] Terrence MacLaren, Trade Secrets Throughout the World, § 29:4 (2012); Paul Sumpter, Intellectual Property Law: Principles in Practice 326 (2006).

PERU

Source of Law, Definition and Scope

Statutory or Other Protection		**Definition**			**Additional Elements of Definition**					**Scope**	
Civil	Criminal	All confidential business information	Common Definition: Confidential business information, **subject to:** deriving value from secrecy; reasonable and making reasonable efforts to maintain secrecy	Common definition **plus condition that** it be imparted to recipient in confidence	Use must be shown	Inventory of trade secrets required	Must be reduced to writing	Must be identified as a trade secret to recipient	Written notice to recipient required	Confidential Business Information	Technical Information
Yes.	Yes.	No.	Yes.	No.	No.	No.	No.	No.	No.	Yes.	Yes.

PERU

Covered Acts

Acts Covered as Civil Infringement		**Acts Covered as Crimes**		**Third Parties:** **Liable for Acquisition?** **Liable Even if Innocent (Without Knowledge)?**	
Breach of Duty?	Wrongful Acquisition / Misappropriation	Breach of Duty?	Wrongful Acquisition/ Misappropriation	Civil	Criminal
Use in Breach of Duty. Disclosure in Breach of Duty.	Yes.	Yes. Criminal sanctions apply only to an employee, a public functionary in charge of guarding the secret, or a person who has a commercial or contractual relationship with the owner of the trade secret.	No.	Yes. No. Knowledge required.	Yes. No. Knowledge required.

PERU

Defining Duties and Misappropriation

Defining Duty of Confidentiality			**Restrictions on Duty of confidentiality**		**Defining Wrongful Acquisition - Misappropriation**	
Commercial Relationship	Current Employment Relationship	Past Employment Relationship	Commercial Relationship	Employment Relationship	Civil	Criminal
Duty can be based on express agreement in commercial contract. Duty can be implied in the context of a business relationship.	Duty can be based on express agreement. Duty is statutorily imposed in the context of an employment relationship.	Express and statutory duty is enforceable, but as per notes below, very hard or impossible to prove.	None.	None.	Espionage or analogous means; inducement of contractual breach.	Not applicable.

PERU

Restrictions on Liability

Additional Elements of Proof in Infringement Claim		**Contractual Restrictions on Competition - Validity**		**Defences**	
Civil	Criminal	Commercial Relationship	Post-Employment	Civil	Criminal
None.	None.	Enforceable, subject to competition law.	Not valid.	Independent creation. Reverse engineering.	Independent creation. Reverse engineering.

PERU

Remedies

Civil Remedies								**Criminal Remedies**		
Preliminary injunction	Permanent injunction	Injunction to eliminate wrongful head start	Delivery up and/or destruction of infringing materials	Compensatory Damages – Availability and Type	Defendant's Profits	Punitive damages available?	Statutory or Pre-established damages	Fines	Jail Sentence	Other
Yes.	Yes.	No.	Yes.	Actual losses. Loss of profit.	No.	No.	No.	60 to 120 days income. 500 000 PEN if profit is obtained.	Up to 2 years.	Restitution and indemnification of damages.

PERU

Enforcement, investigation and discovery & related regulations

Enforcement, investigation and discovery			**Data Exclusivity**		**Technology Transfer**	**Legal Complements**
Emergency Search to preserve and obtain proof	Pre-trial discovery	Protection of confidentiality of trade secrets in litigation	Drugs	Agricultural Chemicals		Fraser Score
No.	Documentary and interrogatories under supervision of court.	General protection. Court secures evidence, protects information from disclosure, prevents unauthorised access.	Five years from approval for new chemical components.	Ten years from approval for new chemical components.	Employer owns employee inventions, but employee has right to compensation for their use. Inbound agreements subject to registration, review, and approval. Substantive restrictions involving trade secrets: No prohibition on exports made using the technology. Less restrictive than in the past.	On the Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, Colombia receives a score of 5.49 out of 10, which ranks it 70th in the world.[115] It scores particularly low on judicial independence (3.08 out of 10).

115 Fraser Institute, Economic Freedom of the World 2010 Annual Report at 127 (2010).

PERU

Additional Comments

Expert characterisation of the operation of the protection of trade secrets in practice
There is extremely limited expert commentary on Peruvian Trade Secret Law. There is no record of criminal enforcement: "There is no available record of enforcement of Article 165 of the Penal Code."[116] "It should be noted that the unlawful disclosure of a secret by a former employee to a new employer, is often hard, if not impossible, to demonstrate in administrative or judicial proceedings."[117] Trade Secrets Throughout the World § 30:14.

SOURCES:
MacLaren, Trade Secrets Throughout the World § 30 (2012).
Adriana Barrera, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, Peru (2010).

116 MacLaren, Trade Secrets Throughout the World § 30:9 (2012).

117 Ibid at § 30:14.

RUSSIAN FEDERATION

Source of Law, Definition and Scope

Statutory or Other Protection		**Definition**			**Additional Elements of Definition**					**Scope**	
Civil	Criminal	All confidential business information	Common Definition: Confidential business information, **subject to:** deriving value from secrecy; reasonable and making reasonable efforts to maintain secrecy	Common definition **plus condition that** it be imparted to recipient in confidence	Use must be shown	Inventory of trade secrets required	Must be reduced to writing	Must be identified as a trade secret to recipient	Written notice to recipient required	Confidential Business Information	Technical Information
Comprehensive civil protection pursuant to statute.	Comprehensive criminal protection pursuant to statute.	No.	Yes.	No.	No.	Yes. (The "regime of secrecy" require-ments described below).	Yes. (The "regime of secrecy" require-ments described below).	Yes. (The "regime of secrecy" require-ments described below).	Yes. (The "regime of secrecy" require-ments described below). In addition, list of recipients and parties with access must be kept.	Yes.	Yes.

RUSSIA

Covered Acts

Acts Covered as Civil Infringement		**Acts Covered as Crimes**		**Third Parties:** **Liable for Acquisition?** **Liable Even if Innocent (Without Knowledge)?**	
Breach of Duty?	Wrongful Acquisition/ Misappropriation	Breach of Duty?	Wrongful Acquisition/ Misappropriation	Civil	Criminal
Yes. *	Yes.*	Yes.* Intentional unauthorized use or disclosure of trade secrets by an employee or other person entrusted with them.	Yes.* Intentionally gathering trade secrets by theft of documents, bribery, threats, or other illegal means.	Yes. No. Only liable if third party has knowledge or reason to know. Innocent third party not liable for damages, but still subject to an injunction.	Yes. No. Knowledge and intent required.

* "Regime of secrecy" requirements limit scope.

RUSSIA

Defining Duties and Misappropriation

Defining Duty of Confidentiality			**Restrictions on Duty of confidentiality**		**Defining Wrongful Acquisition - Misappropriation**	
Commercial Relationship	Current Employment Relationship	Past Employment Relationship	Commercial Relationship	Employment Relationship	Civil	Criminal
Duty can be based on express agreement only, due to regime of secrecy requirements.	Duty can be based on express agreement only, due to regime of secrecy requirements.	Duty can be based on express agreement only, due to regime of secrecy requirements. There is doubt as to whether there is an enforceable duty, at least with a remedy of injunction as discussed below in the final entry regarding expert opinion.	Regime of secrecy requirements described below.	Regime of secrecy requirements described below.	Because trade secrets are IP rights, and infringement does not depend on circumstances of acquisition, *any* knowing appropriation of a trade secret should constitute misappropriation.	Intentionally gathering trade secrets by theft of documents, bribery, threats, or other illegal means.

RUSSIA

Restrictions on Liability

Additional Elements of Proof in Infringement Claim		**Contractual Restrictions on Competition - Validity**		**Defences**	
Civil	Criminal	Commercial Relationship	Post-Employment	Civil	Criminal
Regime of secrecy requirements: (1) trade secrets must be inventoried (and thus reduced to writing); (2) disclosed subject to express agreement; (3) records of those with access kept; (4) all documents marked with secrecy notice that includes owner's address.	Regime of secrecy requirements: (1) trade secrets must be inventoried (and thus reduced to writing); (2) disclosed subject to express agreement; (3) records of those with access kept; (4) all documents marked with secrecy notice that includes owner's address.	Non-competition agreements are becoming more common in practice, but there is little or no case law interpreting their validity as discussed below in the final entry regarding expert opinion.	Non-competition agreements are becoming more common in practice, but there is little or no case law interpreting their validity as discussed below in the final entry regarding expert opinion.	Independent creation.	Independent creation.

RUSSIA

Remedies

Civil Remedies								Criminal Remedies		
Preliminary injunction	Permanent injunction	Injunction to eliminate wrongful head start	Delivery up and/or destruction of infringing materials	Compensatory Damages – Availability and Type	Defendant's Profits	Punitive damages available?	Statutory or Pre-established damages	Fines	Jail Sentence	Other
Yes, but there is doubt as to the practical availability of the remedy of injunction as discussed below in the final entry regarding expert opinion.	Yes (for so long as remains secret) But there is doubt as to the practical availability of the remedy of injunction as discussed below in the final entry regarding expert opinion.	Uncertain.	Yes.	General compensatory damages. Special compensatory damages. Lost profits[118].	Yes.	Yes.	No.	For misappropriation, 80 thousand rubles, or six to twelve months' wages. Unauthorized disclosure 120 thousand rubles or up to twelve months' income.	For misappropriation up to 2 years imprisonment. For unauthorized disclosure, up to 3 years imprisonment.	For unauthorized disclosure, "deprivation of the person of his/her right to occupy certain offices or engage in certain activities for a term of up to three years."[119] For large-scale harm (damages exceeding 250 000 rubles) or are committed with a selfish or mercenary motive, punishment is elevated to a fine of up to 200 000 rubles or 18 months income with "a deprivation of the person of his/her right to occupy certain offices or engage in certain activities for a term of up to five years;" or up to five years imprisonment.

118 But see, Artem Sirota: Major problems of contribution of the rights to the knowhow (trade secret) as an investment in the charter (share) capital of a Russian company, http://www.sirotamosgo.ru/publications/mpc/, April 2011, stating "The remedies for trade secret infringement are limited to direct, real damages incurred as the result of the trade secret infringement. Lost profit cannot be recovered."

119 Article 183, Criminal Code of the Russian Federation No. 63-FZ of June 13, 1996 (as last amended on June 29, 2009), translation available at: http://www.wipo.int/wipolex/en/text.jsp?file_id=202465.

RUSSIA

Enforcement, investigation and discovery & related regulations

Enforcement, investigation and discovery			**Data Exclusivity**		**Technology Transfer**	**Legal Complements**
Emergency Search to preserve and obtain proof	Pre-trial discovery	Protection of confidentiality of trade secrets in litigation	Drugs	Agricultural Chemicals		Fraser Score
Yes. Actions taken may include a search with the participation of the court bailiff and seizure of evidence. Ex parte available.	In practical terms, none.	Full protection with respect to hearings (in camera hearings available). Some protection of documents.	Data submitted for purposes of registering a pharmaceutical cannot be transferred, disclosed, or used for business purposes or for state registration purposes by a third party for six years without the consent of the applicant.[120] This provision is applicable to applications after the date of entry into force of the protocol on Russia's accession to the WTO (2012).	Six years (effective January 2012).	None.	On the Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, Russia receives a score of 5.73 out of 10, which ranks it 64th in the world. It ranks particularly low with respect to judicial independence (2.82 out of 10) and impartial courts (2.98 out of 10), as well as protection of property rights (3.45 out of 10).[121]

120 IP Legislation News, http://www.gorodissky.com/law_news/?newsid=34, 21 August 2012.

121 Ibid.

RUSSIA

Additional Comments

Expert characterisation of the operation of the protection of trade secrets in practice
Expert opinion casts doubt on the practical availability of injunctive relief in trade secret cases. In the case of *OJSC TNK-BP Holding v. Lazurenko*,[122] the English courts found it necessary to apply Russian trade secret law. Expert opinion on Russian law caused the High Court of London to dissolve an injunction granted by the lower court. The expert stated: "[I]t is theoretically possible to seek judicial prohibition to the defendant to undertake particular actions in relation to protected information as an injunctive relief measure under Article 140 of the RF Civil Procedure Code . . . but we are unaware whether the Russian courts have ever granted any such injunction to secure the employer's claim seeking compensation of damages caused by unauthorized disclosure by the employee of the protected information."[123] The London High Court thus concluded: "Accordingly, it is clearly Mr. Rozenberg's view that under Russian law commercially confidential information may not be protected by a quia timet injunction, whether interim or final." This conclusion appears to contradict Article 1252, which provides for a remedy "preventing the actions infringing the right or creating a threat of tis infringement," but also may reflect actual experience.[124] Sources have noted that Russian courts appear to be reluctant to award large amounts of damages.[125]

SOURCES:
See Annex 2 of this paper for a detailed overview of Russia's trade secret law and sources.

122 [2012] EWHC 2781 (Ch).

123 [2012] EWHC 2781 (Ch).

124 See also, Artem Sirota, Major problems of contribution of the rights to the knowhow (trade secret) as an investment in the charter (share) capital of a Russian company, http://www.sirotamosgo.ru/publications/mpc/, April 2011, stating "The remedies for trade secret infringement are limited to direct, real damages incurred as the result of the trade secret infringement. Lost profit cannot be recovered."

125 Damages for breach of contract: a Russian and English law comparison, Practical Law Company Practice Note (2011), http://us.practicallaw.com/6-504-1460; Punitive damages have come to Russia, Russian Law Online (Sept. 24, 2009), http://www.russianlawonline.com/infringement-ip-rights-russia-damages.

SINGAPORE

Source of Law, Definition and Scope

Statutory or Other Protection		**Definition**			**Additional Elements of Definition**					**Scope**	
Civil	Criminal	All confidential business information	Common Definition: Confidential business information, **subject to:** deriving value from secrecy; reasonable and making reasonable efforts to maintain secrecy	Common definition **plus condition that** it be imparted to recipient in confidence	Use must be shown	Inventory of trade secrets required	Must be reduced to writing	Must be identified as a trade secret to recipient	Written notice to recipient required	Confidential Business Information	Technical Information
No statutory protection. Civil protection by means of common law, with reference to English law.	No. (Beyond certain very isolated and specific offenses).	No.	Yes.	No.	No.	No.	No.	No.	No.	Yes, but still follows English case of *Faccenda Chicken*, which provides narrower protection for confidential business information.	Yes.

SINGAPORE

Covered Acts

Acts Covered as Civil Infringement		**Acts Covered as Crimes**		**Third Parties:** **Liable for Acquisition?** **Liable Even if Innocent (Without Knowledge)?**	
Breach of Duty?	Wrongful Acquisition/ Misappropriation	Breach of Duty?	Wrongful Acquisition/ Misappropriation	Civil	Criminal
Use in Breach of Duty. Disclosure in Breach of Duty.	Yes. Although information must generally be imparted in confidence, courts have waived this requirement, at least where defendant engaged in tortious or criminal act to obtain information it could not obtain legally.	No.	No.	Yes. Uncertain whether knowledge required, or at least reason to know. Innocent party may be liable. But in any event, will be restrained after notice.	Not applicable.

SINGAPORE

Defining Duties and Misappropriation

Defining Duty of Confidentiality			**Restrictions on Duty of confidentiality**		**Defining Wrongful Acquisition - Misappropriation**	
Commercial Relationship	Current Employment Relationship	Past Employment Relationship	Commercial Relationship	Employment Relationship	Civil	Criminal
Duty can be based on express agreement in commercial contract. Duty can be implied in the context of a business relationship.	Duty can be based on express agreement. Duty can be implied in the context of an employment relationship. Broad during employment relationship, but limited specifically to trade secrets afterward.	Duty can be based on express contract. Implied duty can continue after employment terminates. No inevitable disclosure doctrine.	Generally valid.	Generally valid, but neither express nor implied post-employment duties to keep information confidential may cover general skills and knowledge.	Yes, at least where defendant engaged in tortious or criminal act.	Not applicable.

SINGAPORE

Restrictions on Liability

Additional Elements of Proof in Infringement Claim		**Contractual Restrictions on Competition - Validity**		**Defences**	
Civil	Criminal	Commercial Relationship	Post-Employment	Civil	Criminal
Detriment must be shown.	Not applicable.	Generally enforceable.	Must be reasonable to protect employers interests and with respect to geographic scope and duration.	Independent creation. Reverse engineering.	Not applicable.

SINGAPORE

Remedies

Civil Remedies								**Criminal Remedies**		
Preliminary injunction	Permanent injunction	Injunction to eliminate wrongful head start	Delivery up and/or destruction of infringing materials	Compensatory Damages – Availability and Type	Defendant's Profits	Punitive damages available?	Statutory or Pre-established damages	Fines	Jail Sentence	Other
Yes. Ex parte available.	Yes. (For so long as remains secret).	Yes.	Yes.	Out of pocket. Lost Profits. Consequential. Defendant's profits.	Yes.	No.	No.	None.	None.	None.

SINGAPORE

Enforcement, investigation and discovery & related regulations

Enforcement, investigation and discovery			**Data Exclusivity**		**Technology Transfer**	**Legal Complements**
Emergency Search to preserve and obtain proof	Pre-trial discovery	Protection of confidentiality of trade secrets in litigation	Drugs	Agricultural Chemicals		Fraser Score
Yes. "Anton Piller" Orders are available. Ex parte available. Independent lawyers conduct search.	Documentary under supervision of court.	Protective orders to prevent disclosure of documents available. In camera proceedings available. However, the details of the secret must be revealed to the court and defendant. But they need not be filed with the pleadings.	Five years from filing date.	Five years from filing date.	None.	On the Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, Malaysia receives a score of 8.38 out of 10, which ranks it 10th in the world.[126]

126 Fraser Institute, Economic Freedom of the World 2010 Annual Report at 137 (2010).

SINGAPORE

Additional Comments

Expert characterisation of the operation of the protection of trade secrets in practice
Publically available commentary on trade secret law in Singapore is sparse. Commentators do note that secrets must be pled with great specificity, which does raise concerns with respect to the security of litigation: The Court in *Johnson Pacific Pte Ltd v. Hogberg Fred Rickard Robin [2004] 4 SLR 200* held that in respect of breach of confidence, the plaintiffs must provide all the particulars sought of the allegations of breach of confidence in their statement of claim as it is only fair that the defendants know the information they are attacked for using. As to secret process that is alleged to be used by the defendant, the Court held that a defendant is entitled to particulars as to what features of the process are alleged to be secret. The court may order an inspection of the process by an expert as a substitute for such particulars with a duty to explain to the expert what elements are claimed to be secret and why. In an action for misuse of trade secrets it is necessary for the plaintiff to specify what secrets are relied upon.[127]

SOURCES:
MacLaren, Trade Secrets Throughout the World § 33 (2012).

[127] MacLaren, Trade Secrets Throughout the World § 33:33 (2012).

SOUTH AFRICA

Source of Law, Definition and Scope

Statutory or Other Protection		**Definition**			**Additional Elements of Definition**					**Scope**	
Civil	Criminal	All confidential business information	Common Definition: Confidential business information, **subject to:** deriving value from secrecy; reasonable and making reasonable efforts to maintain secrecy	Common definition **plus condition that** it be imparted to recipient in confidence	Use must be shown	Inventory of trade secrets required	Must be reduced to writing	Must be identified as a trade secret to recipient	Written notice to recipient required	Confidential Business Information	Technical Information
No statutory protection. Civil protection by means of Roman-Dutch law and common law, pursuant to the Lex Aquilla.	No. (Beyond certain very isolated and specific offenses).	No.	Yes.	No.	No.	No.	No.	No.	No.	Yes.	Yes.

SOUTH AFRICA

Covered Acts

Acts Covered as Civil Infringement		**Acts Covered as Crimes**		**Third Parties:** **Liable for Acquisition?** **Liable Even if Innocent (Without Knowledge)?**	
Breach of Duty?	Wrongful Acquisition/ Misappropriation	Breach of Duty?	Wrongful Acquisition/ Misappropriation	Civil	Criminal
Use in Breach of Duty. Disclosure in Breach of Duty.	Yes. A general action pursuant to the Lex Aquilla.	No.	No.	Yes. No. Knowledge required, or at least reason to know.	Not applicable.

SOUTH AFRICA

Defining Duties and Misappropriation

Defining Duty of Confidentiality			**Restrictions on Duty of confidentiality**		**Defining Wrongful Acquisition - Misappropriation**	
Commercial Relationship	Current Employment Relationship	Past Employment Relationship	Commercial Relationship	Employment Relationship	Civil	Criminal
Duty can be based on express agreement in commercial contract. Duty can be implied in the context of a business relationship.	Duty can be based on express agreement. Duty can be implied in the context of an employment relationship. May not apply to employees with limited discretion and responsibility.	Duty can be based on express contract. Implied duty can continue after employment terminates. Implied duty may not apply to employees with limited discretion and responsibility. No inevitable disclosure doctrine.	Generally valid.	Generally valid, but neither express nor implied post-employment duties to keep information confidential may cover general skills and knowledge.	Torts, crimes, and other improper means. Improper means are actions such as industrial espionage that are "contra bonos mores" (against good morality) and thus violate the Lex Aquilla.	Not applicable.

SOUTH AFRICA

Restrictions on Liability

Additional Elements of Proof in Infringement Claim		**Contractual Restrictions on Competition - Validity**		**Defences**	
Civil	Criminal	Commercial Relationship	Post-Employment	Civil	Criminal
None.	Not applicable.	Valid and enforceable if reasonably necessary to protect valid proprietary interests and not against public policy.	Valid and enforceable if reasonably necessary to protect valid proprietary interests and not against public policy. Reasonableness considered. Factors include duration, geographic area, ability to make a living.	Independent creation Reverse engineering Constitutional right of access to information that is held by another person and that is required for the exercise of protection of any rights. Regulated pursuant to Promotion of Access to Information Act 2/2000.	Not applicable.

SOUTH AFRICA

Remedies

Civil Remedies								**Criminal Remedies**		
Preliminary injunction	Permanent injunction	Injunction to eliminate wrongful head start	Delivery up and/or destruction of infringing materials	Compensatory Damages – Availability and Type	Defendant's Profits	Punitive damages available?	Statutory or Pre-established damages	Fines	Jail Sentence	Other
Yes. Ex parte available.	Yes. (For so long as remains secret).	Yes.	Yes.	Out of pocket. Lost Profits. Consequential. Defendant's profits.	Yes.	No.	No.	None.	None.	None.

SOUTH AFRICA

Enforcement, investigation and discovery & related regulations

Enforcement, investigation and discovery			**Data Exclusivity**		**Technology Transfer**	**Legal Complements**
Emergency Search to preserve and obtain proof	Pre-trial discovery	Protection of confidentiality of trade secrets in litigation	Drugs	Agricultural Chemicals		Fraser Score
Yes. Although some doubt has been cast as to whether "Anton Piller" Orders should be granted under RSA law, they continue to be available. Ex parte available. An official conducts search.	Documentary under supervision of court.	Limited. Protective orders may be available.	No data exclusivity.	No data exclusivity.	Yes. Outbound IP transfer agreements require approval pursuant to a 2012 amendment to the Currency and Exchanges Act 9 of 1933.	On the Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, South Africa receives a score of 6.33 out of 10, which ranks it 46th in the world.[128] It scores particularly low on legal enforcement of contracts (3.93 out of 10).

128 Fraser Institute, Economic Freedom of the World 2010 Annual Report at 140 (2010).

SOUTH AFRICA

Additional Comments

Expert characterisation of the operation of the protection of trade secrets in practice
Publically available commentary on trade secret law in South Africa was sparse. South Africa is undergoing an intellectual property law review process expected to result in reform: "There is currently a review of the entire body of intellectual property law with a view to bringing it in line with international best practice, but also to align it with the strategic planning of Government. This review process, which was announced and commenced at the IP Indaba in August 2012, is closely linked to the drafting of an IP Policy instrument spanning the entire field of IP and its interfaces with other areas of law, and is expected to be continued during 2013. The IP Policy document will be a cross-cutting policy instrument, also taking into account international developments, and will be the outcome of an inclusive consultation process. It is likely to lead to amendments of all IP laws."[129]

SOURCES:
MacLaren, Trade Secrets Throughout the Work § 34 (2012).
Practical Law Company, IP in business transactions: South Africa overview (April, 2013), http://uk.practicallaw.com/6-519-5891#a480193.

[129] Practical Law Company, IP in business transactions: South Africa overview (April, 2013), http://uk.practicallaw.com/6-519-5891#a480193.

SWEDEN

Source of Law, Definition and Scope

Statutory or Other Protection		**Definition**			**Additional Elements of Definition**					**Scope**	
Civil	Criminal	All confidential business information	Common Definition: Confidential business information, **subject to:** deriving value from secrecy; reasonable and making reasonable efforts to maintain secrecy	Common definition **plus condition that** it be imparted to recipient in confidence	Use must be shown	Inventory of trade secrets required	Must be reduced to writing	Must be identified as a trade secret to recipient	Written notice to recipient required	Confidential Business Information	Technical Information
Yes.	Yes.	No.	Yes.	No.	No.	No.	No.	Yes. With respect to employee liability for negligent or intentional breach of duty by disclosure.	No.	Yes.	Yes.

SWEDEN

Covered Acts

Acts Covered as Civil Infringement		**Acts Covered as Crimes**		**Third Parties:** **Liable for Acquisition?** **Liable Even if Innocent (Without Knowledge)?**	
Breach of Duty?	Wrongful Acquisition/ Misappropriation	Breach of Duty?	Wrongful Acquisition/ Misappropriation	Civil	Criminal
Yes. Attempt also covered.	Yes. Very broad. See definition below. Attempt also covered.	No. The criminal sections only cover unauthorized access, so according to case law, an employee or other with a duty, and thus, authorized access, cannot be liable.	Yes. Very broad. So long as information meets the definition of a trade secret, then unauthorized access constitutes an act of criminal infringement. Attempt also covered.	Yes. No. Only liable if third party has knowledge or reason to know.	Yes. No. Only liable with knowledge.

SWEDEN

Defining Duties and Misappropriation

Defining Duty of Confidentiality			**Restrictions on Duty of confidentiality**		**Defining Wrongful Acquisition - Misappropriation**	
Commercial Relationship	Current Employment Relationship	Past Employment Relationship	Commercial Relationship	Employment Relationship	Civil	Criminal
Intentionally or negligently exploiting or disclosing a trade secret without authorization, where that trade secret was learned in confidence in connection with a business transaction. (Article 6).	Intentionally or negligently exploiting or disclosing a trade secret without authorization, where that trade secret was learned through employment. The employee must be informed it is secret and must know or ought to know that he is not authorized to reveal it. (Article 7).	Implied duty does not continue, except in exceptional circumstances – where employee gathers trade secrets for use after employment. An express contract remains in force, but a court will consider whether the agreement is equitable.	None.	Court will determine reasonableness, which includes duration. If the provision is unlimited in duration, it may be consider inequitable and held void or modified. Courts will also exclude knowledge that has become part of an employee's general skills and knowledge.	Any intentional access of a trade secret without authorization. Intentional or negligent use or disclosure of a trade secret that was disclosed in breach of duty or wrongfully obtained.	Any intentional access of a trade secret without authorization. Obtaining trade secrets with knowledge that they were previously wrongfully accessed.

SWEDEN

Restrictions on Liability

Additional Elements of Proof in Infringement Claim		**Contractual Restrictions on Competition - Validity**		**Defences**	
Civil	Criminal	Commercial Relationship	Post-Employment	Civil	Criminal
None.	None.	Commercial agreements not to compete generally enforceable, subject to competition regulations.	Covenants not to compete are scrutinized carefully to determine whether they are inequitable. Such agreements must be necessary and reasonable with respect to accomplishing their purpose. Factors to be considered include the specific purpose to be accomplished, with protecting a trade secret (but not the employee's general skill and knowledge) as one of the permissible purposes. Duration and geographic scope are relevant to reasonableness as well.	Independent creation.	Independent creation.

SWEDEN

Remedies

Civil Remedies								Criminal Remedies		
Preliminary injunction	Permanent injunction	Injunction to eliminate wrongful head start	Delivery up and/or destruction of infringing materials	Compensatory Damages – Availability and Type	Defendant's Profits	Punitive damages available?	Statutory or Pre-established damages	Fines	Jail Sentence	Other
Yes.	Yes.	Uncertain.	Yes.	Out of pocket. Lost Profits. Damages sufficient to ensure that infringement is not profitable.	Yes.	No.	No.	None.	Up to 2 years for accessing without authorization; 6 years in egregious cases. For obtaining trades secrets with knowledge they were previously wrongfully accede, up to 2 years; 4 years in egregious cases.	Civil liability under Article 5 of the Trade Secrets Act for violation of the criminal Articles of the Act.

SWEDEN

Enforcement, investigation and discovery & related regulations

Enforcement, investigation and discovery			**Data Exclusivity**		**Technology Transfer**	**Legal Complements**
Emergency Search to preserve and obtain proof	Pre-trial discovery	Protection of confidentiality of trade secrets in litigation	Drugs	Agricultural Chemicals	Civil	Fraser Score
None in civil cases. Available to prosecutors in criminal cases.	Limited discovery of documents and physical evidence under supervision of court.	Partial protection with respect to hearings. No protection from other party. Record may be sealed. Secrecy is at discretion of court, court's order, if it comes, may be after some delay with secrets unprotected. Criticized by commenters as insufficient. See below.	"8 + 2 + 1 year approach." Pharmaceutical test data submitted to government for new medicinal products and new indications or uses is protected from disclosure or use for 8 years. Once the 8 year period ends, the data can be used by generic manufacturers to prepare and apply for regulatory approval, but not market a product. This period of market exclusivity lasts 2 years. The initial applicant may receive another 1 year for new indications.	"8 + 2 + 1 year approach." Test data submitted to government for new products and new indications or uses is protected from disclosure or use for 8 years. Once the 8 year period ends, the data can be used by generic manufacturers to prepare and apply for regulatory approval, but not market a product. This period of market exclusivity lasts 2 years. The initial applicant may receive another 1 year for new indications.	None.	On the Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, Sweden receives a score of 8.47 out of 10, which ranks it 6th in the world.

SWEDEN

Additional Comments

Expert characterisation of the operation of the protection of trade secrets in practice
The law is considered comprehensive and relatively effective. It offers Europe's most comprehensive set of statutory provisions dedicated to the protection of trade secrets. Nevertheless, commentators do observe some deficiencies in the current Trade Secrets Act. A 2008 Legislative Committee report noted two deficiencies.[130] First, the criminal provisions of the Act do not apply to a party that originally has lawful access to a secret—for example, an employee who discloses trade secrets. Second, the Act does not yet fully implement the EU Enforcement Directive to allow parties to seek an emergency search of an alleged infringer's premises to secure evidence. Other observers have contended that the litigation process needs to be made more secure. A recent report prepared by the consultants for the EU contended that: > The protection of trade secrets is insufficient in respect of information obtained by a party during court proceedings in general courts. A new rule on liability for damages should be added so that anyone who, without valid cause, discloses or commercially exploits trade secrets obtained in court proceedings may be liable for damages.[131]

SOURCES:
See Annex 2 of this paper for a detailed overview of Sweden's trade secret law and sources.

130 Marianne Levin et al., Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, Sweden 13 (2010).

131 Hogan Lovells Report, Appendix 3 at 63 (2012).

UNITED KINGDOM

Source of Law, Definition and Scope

Statutory or Other Protection		**Definition**			**Additional Elements of Definition**					**Scope**	
Civil	Criminal	All confidential business information	Common Definition: Confidential business information, **subject to:** deriving value from secrecy; reasonable and making reasonable efforts to maintain secrecy	Common definition **plus condition that** it be imparted to recipient in confidence	Use must be shown	Inventory of trade secrets required	Must be reduced to writing	Must be identified as a trade secret to recipient	Written notice to recipient required	Confidential Business Information	Technical Information
Comprehensive civil protection by means of common law.	No.	No.	Yes.	This condition appears to have been abandoned.	No.	No.	No.	No.	No.	Yes.	Yes. (Most likely so since *Lansing Linde Ltd v Kerr*, [1991] 1 W.L.R. 251).

UNITED KINGDOM

Covered Acts

Acts Covered as Civil Infringement		**Acts Covered as Crimes**		**Third Parties: Liable for Acquisition? Liable Even if Innocent (Without Knowledge)?**	
Breach of Duty?	Wrongful Acquisition/ Misappropriation	Breach of Duty?	Wrongful Acquisition/ Misappropriation	Civil	Criminal
Use in Breach of Duty. Disclosure in Breach of Duty.	Yes, but based on duty implied from the circumstances. Court will imply a duty of confidentiality where the party acquiring the information knows or should know that the information is intended to be kept private.	Not applicable.	Not applicable.	Yes. No. Only liable if third party has knowledge. However, liability does apply where the third party later comes to know that the information was disclosed in breach of duty.	Not applicable.

UNITED KINGDOM

Defining Duties and Misappropriation

Defining Duty of Confidentiality			**Restrictions on Duty of confidentiality**		**Defining Wrongful Acquisition - Misappropriation**	
Commercial Relationship	Current Employment Relationship	Past Employment Relationship	Commercial Relationship	Employment Relationship	Civil	Criminal
Duty can be based on express agreement in commercial contract. Duty can be implied in the context of a business relationship.	Duty can be based on express agreement and implied duty. Implied duty broad during employment – covers information beyond strict trade secret definition.	Duty can be based on express contract. Duty is also implied. Implied duty narrower after employment – only trade secrets. No inevitable disclosure doctrine.	None.	Express agreements may cover general skills and knowledge. Implied post-employment duties to keep information confidential likely unenforceable with respect to general skills and knowledge.	Based on duty implied from the circumstances. Court will imply a duty of confidentiality where the party acquiring the information knows or should know that the information is intended to be kept private.	Not applicable.

UNITED KINGDOM

Remedies

Civil Remedies								**Criminal Remedies**		
Preliminary injunction	Permanent injunction	Injunction to eliminate wrongful head start	Delivery up and/or destruction of infringing materials	Compensatory Damages – Availability and Type	Defendant's Profits	Punitive damages available?	Statutory or Pre-established damages	Fines	Jail Sentence	Other
Yes.	Yes. (For so long as remains secret).	Yes, even where information has since become public.	Yes.	Out of pocket. Lost Profits. Consequential. Defendant's profits.	Yes.	No.	No.	Not applicable.	Not applicable.	Not applicable.

UNITED KINGDOM

Enforcement, investigation and discovery & related regulations

Enforcement, investigation and discovery			**Data Exclusivity**		**Technology Transfer**	**Legal Complements**
Emergency Search to preserve and obtain proof	Pre-trial discovery	Protection of confidentiality of trade secrets in litigation	Drugs	Agricultural Chemicals	Civil	Fraser Score
Yes. "Anton Piller" Order. Ex parte available. Plaintiff may conduct search. Level of proof greater than for preliminary injunction.	Documentary. At initiative of party.	Full protection with respect to hearings (in camera hearings available). Protection from other party available (protective orders, measures limiting viewing to counsel or other professionals).	"8 + 2 + 1 year approach." Pharmaceutical test data submitted to government for new medicinal products and new indications or uses is protected from disclosure or use for 8 years. Once the 8 year period ends, the data can be used by generic manufacturers to prepare and apply for regulatory approval, but not market a product. This period of market exclusivity lasts 2 years. The initial applicant may receive another 1 year for new indications.	"8 + 2 + 1 year approach." Test data submitted to government for new products and new indications or uses is protected from disclosure or use for 8 years. Once the 8 year period ends, the data can be used by generic manufacturers to prepare and apply for regulatory approval, but not market a product. This period of market exclusivity lasts 2 years. The initial applicant may receive another 1 year for new indications.	None.	On the Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, United Kingdom receives a score of 8.11 out of 10, which ranks it 15th in the world.

UNITED KINGDOM

Additional Comments

Expert characterisation of the operation of the protection of trade secrets in practice
While the protections that exist are considered to be effective with respect to the subject matter they address,[132] there are notable uncertainties regarding scope, subject matter, and remedies. These limitations, together with the absence of criminal provisions, lead some commentators to describe UK trade secret protection as "relatively weak."[133] In recent decades, there have been a number of unanswered calls to strengthen UK trade secret law, including notable reports by the UK Law Commission (a statutory independent body) in 1981 that urged the adoption of a civil statute[134] and in 1997 that urged the adoption of a criminal statute.[135]

SOURCES:
See Annex 2 of this paper for a detailed overview of the United Kingdom's trade secret law and sources.

132 Hogan Lovells Report, Appendix 3 at 68.

133 Adrian Toutoungi, Trade Secrets Move (Slowly) Up the Agenda, Eversheds International Website, (16 August, 2012) available at: http://www.eversheds.com/global/en/what/articles/index.page?ArticleID=en/Industrial_engineering/Trade_secrets_move-slowly-up_the_agenda

134 UK Law Commission, Report on Breach of Confidence (Law Com No.110), (October, 1981).

135 UK Law Commission, Misuse of Trade Secrets Consultation Paper (November, 1997): http://lawcommission.justice.gov.uk/docs/cp150_Legislating_the_Criminal_Code__Misuse_of_Trade_Secrets_Consultation.pdf

UNITED STATES

Source of Law, Definition and Scope

Statutory or Other Protection		**Definition**			**Additional Elements of Definition**					**Scope**	
Civil	Criminal	All confidential business information	Common Definition: Confidential business information, **subject to:** deriving value from secrecy; reasonable and making reasonable efforts to maintain secrecy	Common definition **plus condition that** it be imparted to recipient in confidence	Use must be shown	Inventory of trade secrets required	Must be reduced to writing	Must be identified as a trade secret to recipient	Written notice to recipient required	Confidential Business Information	Technical Information
Comprehen-sive civil protection pursuant to statute.	Comprehen-sive criminal protection pursuant to statute.	No.	Yes.	No.	No.	No.	No.	No.	No.	Yes.	Yes.

UNITED STATES

Covered Acts

Acts Covered as Civil Infringement		**Acts Covered as Crimes**		**Third Parties:** **Liable for Acquisition?** **Liable Even if Innocent (Without Knowledge)?**	
Breach of Duty?	Wrongful Acquisition/ Misappropriation	Breach of Duty?	Wrongful Acquisition/ Misappropriation	Civil	Criminal
Yes.	Yes.	Yes.	Yes.	Yes. No. Only liable if third party has knowledge or reason to know.	Yes. No. Only liable if third party has knowledge or reason to know.

UNITED STATES

Defining Duties and Misappropriation

Defining Duty of Confidentiality			**Restrictions on Duty of confidentiality**		**Defining Wrongful Acquisition - Misappropriation**	
Commercial Relationship	Current Employment Relationship	Past Employment Relationship	Commercial Relationship	Employment Relationship	Civil	Criminal
Duty can be based on express contract or implied.	Duty can be based on express contract or implied.	Duty can be based on express agreement or implied. In some US states, the doctrine of inevitable disclosure exists.	None beyond ordinary competition law concerns. Ends with public disclosure of confidential information.	Ends with public disclosure of confidential information.	Obtaining secrets by tort, crime, espionage, or other act that circumvents reasonable security measures.	1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information; (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information; (3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization; (4) attempts to commit any offense described in paragraphs (1) - (3); or (5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy . . . .[136]

[136] 18 USC § 1832 (2013).

UNITED STATES

Restrictions on Liability

Additional Elements of Proof in Infringement Claim		**Contractual Restrictions on Competition - Validity**		**Defences**	
Civil	Criminal	Commercial Relationship	Post-Employment	Civil	Criminal
None.	None.	Per se prohibited in some states. If not, must be related to the protection of trade secrets, limited in duration and geographic scope.	Per se prohibited in some states. If not, must be related to the protection of trade secrets, limited in duration and geographic scope.	Independent creation. Reverse engineering.	Independent creation. Reverse engineering.

UNITED STATES

Remedies

Civil Remedies								Criminal Remedies		
Preliminary injunction	Permanent injunction	Injunction to eliminate wrongful	Delivery up and/or destruction of infringing	Compensatory Damages – Availability and Type	Defendant's Profits	Punitive damages available?	Statutory or Pre-established damages	Fines	Jail Sentence	Other
Yes. Temporary restraining orders and other ex parte action available.	Yes (For so long as remains secret).	Uncertain.	Yes.	Direct. Consequential. Lost Profits.	Yes.	Yes.	No.	In the case of trade secret theft performed to "benefit any foreign government, foreign instrumentality, or foreign agent," an individual may receive up to a USD 5 million fine and up to a 15 year prison sentence, or both."[137] "In the case of an organization, it may receive a fine of up to USD 10 million or "3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided."[138] In the case of more ordinary trade secret appropriation, such as between firms, the Economic Espionage imposes slightly less stringent penalties. It provides that individuals can receive up to a 10 years prison sentence or a fine (the amount is unspecified).[139] Organizations can be fined up to USD 5 million.[140]	See previous cell.	

137 18 U.S.C. § 1831(a).
138 18 USC § 1831(b).

UNITED STATES

Enforcement, investigation and discovery & related regulations

Enforcement, investigation and discovery			**Data Exclusivity**		**Technology Transfer**	**Legal Complements**
Emergency Search to preserve and obtain proof	Pre-trial discovery	Protection of confidentiality of trade secrets in litigation	Drugs	Agricultural Chemicals		Fraser Score
Yes. Ex parte available.	Most extensive in world. Documentary, interrogatories, depositions.	In camera hearings available. Protection of documents available. Protection from other party available.	5 years for new chemical entities. 3 years for new clinical investigation 12 years for biologics	10 years for agricultural chemical products, if new chemical entity. For new uses and indications, additional 5 year period of data compensability.	None.	On the Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, the US receives a score of 7.5 out of 10, which ranks it 22nd in the world.[141]

139 18 U.S.C. § 1832(a).

140 18 U.S.C. § 1832 (b).

141 Fraser Institute, Economic Freedom of the World 2010 Annual Report at 166 (2010).

UNITED STATES

Additional Comments

Expert characterisation of the operation of the protection of trade secrets in practice
Criticism of the US system of trade secret protection is relatively limited. However, there have been recent calls for a national civil cause of action to replace or supplement the laws of the 50 states, which almost all adopted the Uniform Trade Secrets Act.[142]

SOURCES:
See Annex 2 of this paper for a detailed overview of the United States' trade secret law and sources.

142 See, e.g. The Report on the US Commission on the Theft of Intellectual Property (2013).

Annex Table

Annex Table A1. Trade Secret Protection Index, by Country, 2010, Panel A (See the notes at the bottom of the table.)

Components and scoring	Score range	Normalised range	Australia	Brazil	Bulgaria	China	Colombia	France	Germany
1. Definition and coverage	**0-12**	**0-1**	**0.71**	**0.83**	**0.50**	**0.67**	**0.92**	**0.83**	**0.92**
a) Scope									
• If scope covers all confidential business information, subject to: 1) deriving value from secrecy and 2) the owner's reasonable efforts to maintain secrecy, score = 1; If scope also subject to requirement that information is imparted to the recipient in confidence, score = ½	0,1		0.5	1	1	1	1	1	1
b) Additional Elements of Definition									
• Inventory of trade secrets required (requirement=0; no requirement=1)	0,1		1	1	1	1	1	1	1
• Must be reduced to writing (requirement=0; no requirement=1)	0,1		1	1	1	0	1	1	1
• Must be identified as a trade secret to recipient (requirement=0; no requirement=1)	0,1		1	1	0	0	1	1	1
• Written notice to recipient required (requirement=0; no requirement=1)	0,1		1	1	0	0	1	1	1
c) Acts covered as civil infringement:									
• Breach of duty (not covered=0, partially covered=½, covered=1)	0,1		1	0.5	1	1	1	1	1
• Wrongful acquisition or misappropriation (not covered=0, partially covered= ½, covered=1)	0,1		1	1	1	1	1	0.5	1
• Third party liability for acquisition with knowledge or reason to know (not available=0, available=1)	0,1		1	1	1	1	1	1	1
• Third party liability for acquisition without knowledge - enjoin "innocent parties" (not available=0, available=1)	0,1		1	0	0	0	0	0	0
d) Acts covered by criminal law									
• Breach of duty (not covered=0, partially covered=½, covered=1)	0,1		0	0.5	0	1	1	1	1
• Wrongful acquisition or misappropriation (not covered=0, partially covered=½, covered=1)	0,1		0	1	0	1	1	0.5	1
• Third party liability for acquisition with knowledge or reason to know (not available=0, available=1)	0,1		0	1	0	1	1	1	1
• Third party liability for acquisition without knowledge, enjoin "innocent parties" (not available=0, available=1)	0,1		0	0	0	0	0	0	0
2. Duties and misappropriation	**0-5**	**0-1**	**1**	**0.8**	**0.6**	**0.6**	**0.9**	**0.9**	**0.9**
• Commercial relationship (covered if arising from: express agreement ½ + implied duty ½)	0,1		1	1	1	0.5	1	0.5	1
• Current employment relationship (covered if arising from: express agreement ½ + implied duty ½)	0,1		1	1	1	0.5	1	1	1
• Past employment relationship (covered if arising from: express agreement ½ + implied duty ½)	0,1		1	1	0	0.5	0.5	1	1
• Restrictions on post-relationship duty of confidentiality (score if no restrictions on matters beyond general skills and knowledge, by relationship: commercial ½ + employment ½)	0,1		1	0.5	0.5	1	1	1	1
• Validity of contractual restrictions on competition (if unenforceable=0; significant limitations=½ (e.g., limited by time or place for either commercial or post-employment situations); generally enforceable=1)	0,1		1	0.5	0.5	0.5	1	1	0.5

Annex Table A1. Trade Secret Protection Index, by Country, 2010, Panel A (continued)

Components and scoring	Score range	Normalised range	Austra-lia	Brazil	Bulgaria	China	Colombia	France	Germ-any
3. Remedies and restrictions on liability	**0-11**	**0-1**	**0.64**	**0.86**	**0.36**	**0.55**	**0.55**	**0.64**	**0.73**
a) Restrictions on liability									
• Additional elements of proof in infringement claims (if none: civil=½ + criminal=½ point; score 1 if there is no criminal law and civil score is ½)	0,1		1	1	1	0	1	1	1
b) Civil remedies									
• Preliminary injunction (if available = 1, if not = 0)	0,1		1	1	1	0	1	1	1
• Ex parte action available under preliminary injunction (if available = 1, if not = 0)	0,1		0	1	0	0	0	0	0
• Permanent injunction (if available = 1, if not = 0)	0,1		1	1	1	1	1	1	1
• Injunction to eliminate wrongful head start (if available = 1, if not = 0)	0,1		1	0	0	0	0	0	0
• Delivery or destruction of infringing materials (if available = 1, if not = 0)	0,1		1	1	0	1	0	1	1
• Compensatory damages (direct or out of pocket damages or consideration of profits or other damages= 1)	0,1		1	1	1	1	1	1	1
• Yielding of defendant's profits (if available = 1, if not = 0)	0,1		1	1	0	1	0	0	1
• Availability of punitive or statutory damages (if available = 1, if not = 0)	0,1		0	1	0	0	0	0	0
c) Criminal remedies									
• Fines, damages or loss of assets (if not available = 0, if minimal per expert opinion= ½, if substantial = 1)	0,1		0	0.5	0	1	1	1	1
• Jail sentence (if available = 1, if not = 0)	0,1		0	1	0	1	1	1	1
4. Enforcement, investigation and discovery; data exclusivity	**0-6**	**0-1**	**0.86**	**0.75**	**0.92**	**0.55**	**0.39**	**0.75**	**0.58**
• Emergency search to preserve and obtain proof (unavailable=0; available but with significant restrictions= ½ (e.g., conducted solely by an official or 3rd party expert); readily available=1)	0,1		1	1	1	0.5	0	0.5	0.5
• Ex parte emergency search availability (unavailable=0, available but with significant restrictions=½, readily available=1)	0,1		1	1	1	1	0	1	0
• Pre-trial discovery (unavailable=0, documentary only or strict limitations = ½, ready availability of documentary and interrogatories = 1)	0,1		0.5	0.5	0.5	0	1	0.5	0
• Protection of confidentiality of trade secrets in litigation (none=0, partial= ½, fully available=1)	0,1		1	1	1	0.5	0	0.5	1
b) Data exclusivity									
• Drugs (years: 0=0; 0.1-3=1/3; 3.1-7.9=2/3; >8=1)	0,1		0.66	0	1	0.66	0.66	1	1
• Agricultural chemicals (years: 0=0, 0.1-4.9=1/3, 5-8=2/3; > 8=1)	0,1		1	1	1	0.66	0.66	1	1
5. System functioning and related regulation	**0-4**	**0-1**	**0.84**	**0.13**	**0.63**	**0.16**	**0.49**	**0.68**	**0.71**
• Technology transfer: registration requirement (none=1; one or more = 0)	0,1		1	0	1	0	0	1	1
• Technology transfer: substantive review or regulation (none=1; one or more = 0)	0,1		1	0	1	0	1	1	1
• Fraser Institute score for *Legal System and Security of Property Rights* (score ranging from 0 to 10, divided by 10)	0,1		0.87	0.52	0.5	0.62	0.44	0.73	0.82
• Expert characterisation of the operation of the protection in practice (NB, based on internationally recognised or peer-reviewed sources; see country charts for details) (Generally negative = 0; none = ½; generally positive = 1)	0,1		0.5	0	0	0	0.5	0	0
Index Total (Sum of the normalised scores for the 5 categories in bold)		**0-5**	**4.05**	**3.38**	**3.01**	**2.52**	**3.23**	**3.80**	**3.83**

Annex Table A1. Trade Secret Protection Index, by Country, 2010, Panel B

Components and scoring	Score range	Normalised range	India	Israel	Italy	Japan	Korea	Malaysia	New Zealand
1. Definition and coverage	**0-12**	**0-1**	**0.54**	**0.71**	**0.75**	**0.92**	**0.83**	**0.54**	**0.67**
a) Scope									
• If scope covers all confidential business information, subject to: 1) deriving value from secrecy and 2) the owner's reasonable efforts to maintain secrecy, score = 1; If scope also subject to requirement that information is imparted to the recipient in confidence, score = ½	0,1		0.5	1	1	1	1	0.5	0.5
b) Additional Elements of Definition									
• Inventory of trade secrets required (requirement=0; no requirement=1)	0,1		1	1	1	1	1	1	1
• Must be reduced to writing (requirement=0; no requirement=1)	0,1		1	1	1	1	1	1	1
• Must be identified as a trade secret to recipient (requirement=0; no requirement=1)	0,1		1	1	1	1	1	1	1
• Written notice to recipient required (requirement=0; no requirement=1)	0,1		1	1	1	1	1	1	1
c) Acts covered as civil infringement:									
• Breach of duty (not covered=0, partially covered=½, covered=1)	0,1		1	1	1	1	1	1	1
• Wrongful acquisition or misappropriation (not covered=0, partially covered= ½, covered=1)	0,1		0	1	1	1	1	0	0
• Third party liability for acquisition with knowledge or reason to know (not available=0, available=1)	0,1		1	1	1	1	1	1	1
• Third party liability for acquisition without knowledge - enjoin "innocent parties" (not available=0, available=1)	0,1		0	0	0	0	0	0	0
d) Acts covered by criminal law									
• Breach of duty (not covered=0, partially covered=½, covered=1)	0,1		0	0	1	1	1	0	0
• Wrongful acquisition or misappropriation (not covered=0, partially covered=½, covered=1)	0,1		0	0.5	0	1	1	0	0.5
• Third party liability for acquisition with knowledge or reason to know (not available=0, available=1)	0,1		0	0	0	1	0	0	1
• Third party liability for acquisition without knowledge, enjoin "innocent parties" (not available=0, available=1)	0,1		0	0	0	0	0	0	0
2. Duties and misappropriation	**0-5**	**0-1**	**0.9**	**1**	**0.9**	**1**	**1**	**0.8**	**1**
• Commercial relationship (covered if arising from: express agreement ½ + implied duty ½)	0,1		1	1	1	1	1	1	1
• Current employment relationship (covered if arising from: express agreement ½ + implied duty ½)	0,1		1	1	1	1	1	1	1
• Past employment relationship (covered if arising from: express agreement ½ + implied duty ½)	0,1		1	1	1	1	1	1	1
• Restrictions on post-relationship duty of confidentiality (score if no restrictions on matters beyond general skills and knowledge, by relationship: commercial ½ + employment ½)	0,1		1	1	1	1	1	1	1
• Validity of contractual restrictions on competition (if unenforceable=0; significant limitations=½ (e.g., limited by time or place for either commercial or post-employment situations); generally enforceable=1)	0,1		0.5	1	0.5	1	1	0	1

Annex Table A1. Trade Secret Protection Index, by Country, 2010, Panel B (continued)

Components and scoring	Score range	Normalised range	India	Israel	Italy	Japan	Korea	Malaysia	New Zealand
3. Remedies and restrictions on liability	**0-11**	**0-1**	**0.73**	**0.64**	**0.77**	**0.82**	**0.82**	**0.68**	**0.77**
a) Restrictions on liability									
• Additional elements of proof in infringement claims (if none: civil=½ + criminal=½ point; score 1 if there is no criminal law and civil score is ½)	0,1		1	1	1	1	1	0.5	0.5
b) Civil remedies									
• Preliminary injunction (if available = 1, if not = 0)	0,1		1	1	1	1	1	1	1
• Exparte action available under preliminary injunction (if available = 1, if not = 0)	0,1		1	0	0	0	0	1	0
• Permanent injunction (if available = 1, if not = 0)	0,1		1	1	1	1	1	1	1
• Injunction to eliminate wrongful head start (if available = 1, if not = 0)	0,1		1	1	1	1	1	1	1
• Delivery or destruction of infringing materials (if available = 1, if not = 0)	0,1		1	1	1	1	1	1	1
• Compensatory damages (direct or out of pocket damages or consideration of profits or other damages= 1)	0,1		1	1	1	1	1	1	1
• Yielding of defendant's profits (if available = 1, if not = 0)	0,1		1	1	1	1	1	1	1
• Availability of punitive or statutory damages (if available = 1, if not = 0)	0,1		0	0	0	0	0	0	1
c) Criminal remedies									
• Fines, damages or loss of assets (if not available = 0, if minimal per expert opinion= ½, if substantial = 1)	0,1		0	0	0.5	1	1	0	0
• Jail sentence (if available = 1, if not = 0)	0,1		0	0	1	1	1	0	1
4. Enforcement, investigation and discovery; data exclusivity	**0-6**	**0-1**	**0.64**	**0.86**	**0.83**	**0.67**	**0.44**	**0.80**	**0.80**
• Emergency search to preserve and obtain proof (unavailable=0; available but with significant restrictions= ½ (e.g., conducted solely by an official or 3rd party expert); readily available=1)	0,1		0.5	0.5	1	0.5	0	1	1
• Ex parte emergency search availability (unavailable=0, available but with significant restrictions=½, readily available=1)	0,1		1	1	1	0	0	1	1
• Pre-trial discovery (unavailable=0, documentary only or strict limitations = ½, ready availability of documentary and interrogatories = 1)	0,1		1	1	0.5	0.5	0.5	0.5	0.5
• Protection of confidentiality of trade secrets in litigation (none=0, partial= ½, fully available=1)	0,1		1	1	0.5	1	0.5	1	1
b) Data exclusivity									
• Drugs (years: 0=0; 0.1-3=1/3; 3.1-7.9=2/3; >8=1)	0,1		0	0.66	1	1	0.66	0.66	0.66
• Agricultural chemicals (years: 0=0, 0.1-4.9=1/3, 5-8=2/3; > 8=1)	0,1		0.33	1	1	1	1	0.66	0.66
5. System functioning and related regulation	**0-4**	**0-1**	**0.15**	**0.90**	**0.64**	**0.94**	**0.80**	**0.78**	**0.85**
• Technology transfer: registration requirement (none=1; one or more = 0)	0,1		0	1	1	1	1	1	1
• Technology transfer: substantive review or regulation (none=1; one or more = 0)	0,1		0	1	1	1	1	1	1
• Fraser Institute score for *Legal System and Security of Property Rights* (score ranging from 0 to 10, divided by 10)	0,1		0.59	0.59	0.57	0.75	0.68	0.62	0.9
• Expert characterisation of the operation of the protection in practice (NB, based on internationally recognised or peer-reviewed sources; see country charts for details) (Generally negative = 0; none = ½; generally positive = 1)	0,1		0	1	0	1	0.5	0.5	0.5
Index Total (Sum of the normalised scores for the 5 categories in bold)		**0-5**	**2.95**	**4.10**	**3.90**	**4.34**	**3.89**	**3.61**	**4.09**

Annex Table A1. Trade Secret Protection Index, by Country, 2010, Panel C

Components and scoring	Score range	Normalised range	Peru	Russia	Singa-pore	South Africa	Sweden	United Kingdom	United States
1. Definition and coverage	**0-12**	**0-1**	**0.83**	**0.58**	**0.75**	**0.67**	**0.75**	**0.67**	**0.92**
a) Scope									
• If scope covers all confidential business information, subject to: 1) deriving value from secrecy and 2) the owner's reasonable efforts to maintain secrecy, score = 1; If scope also subject to requirement that information is imparted to the recipient in confidence, score = ½	0,1		1	1	1	1	1	1	1
b) Additional Elements of Definition									
• Inventory of trade secrets required (requirement=0; no requirement=1)	0,1		1	0	1	1	1	1	1
• Must be reduced to writing (requirement=0; no requirement=1)	0,1		1	0	1	1	1	1	1
• Must be identified as a trade secret to recipient (requirement=0; no requirement=1)	0,1		1	0	1	1	0	1	1
• Written notice to recipient required (requirement=0; no requirement=1)	0,1		1	0	1	1	1	1	1
c) Acts covered as civil infringement:									
• Breach of duty (not covered=0, partially covered=½, covered=1)	0,1		1	1	1	1	1	1	1
• Wrongful acquisition or misappropriation (not covered=0, partially covered= ½, covered=1)	0,1		1	1	1	1	1	1	1
• Third party liability for acquisition with knowledge or reason to know (not available=0, available=1)	0,1		1	1	1	1	1	1	1
• Third party liability for acquisition without knowledge - enjoin "innocent parties" (not available=0, available=1)	0,1		0	0	1	0	0	0	0
d) Acts covered by criminal law									
• Breach of duty (not covered=0, partially covered=½, covered=1)	0,1		1	1	0	0	0	0	1
• Wrongful acquisition or misappropriation (not covered=0, partially covered=½, covered=1)	0,1		0	1	0	0	1	0	1
• Third party liability for acquisition with knowledge or reason to know (not available=0, available=1)	0,1		1	1	0	0	1	0	1
• Third party liability for acquisition without knowledge, enjoin "innocent parties" (not available=0, available=1)	0,1		0	0	0	0	0	0	0
2. Duties and misappropriation	**0-5**	**0-1**	**0.8**	**0.5**	**1**	**1**	**0.7**	**1**	**0.9**
• Commercial relationship (covered if arising from: express agreement ½ + implied duty ½)	0,1		1	0.5	1	1	0.5	1	1
• Current employment relationship (covered if arising from: express agreement ½ + implied duty ½)	0,1		1	0.5	1	1	0.5	1	1
• Past employment relationship (covered if arising from: express agreement ½ + implied duty ½)	0,1		0.5	0.5	1	1	0.5	1	1
• Restrictions on post-relationship duty of confidentiality (score if no restrictions on matters beyond general skills and knowledge, by relationship: commercial ½ + employment ½)	0,1		1	0	1	1	1	1	1
• Validity of contractual restrictions on competition (if unenforceable=0; significant limitations=½ (e.g., limited by time or place for either commercial or post-employment situations); generally enforceable=1)	0,1		0.5	1	1	1	1	1	0.5

Annex Table A1. Trade Secret Protection Index, by Country, 2010, Panel C (continued)

Components and scoring	Score range	Normalised range	Peru	Russia	Singa-pore	South Africa	Sweden	United Kingdom	United States
3. Remedies and restrictions on liability	**0-11**	**0-1**	**0.64**	**0.82**	**0.68**	**0.73**	**0.73**	**0.59**	**1.00**
a) Restrictions on liability									
• Additional elements of proof in infringement claims (if none: civil=½ + criminal=½ point; score 1 if there is no criminal law and civil score is ½)	0,1		1	0	0.5	1	1	0.5	1
b) Civil remedies									
• Preliminary injunction (if available = 1, if not = 0)	0,1		1	1	1	1	1	1	1
• Ex parte action available under preliminary injunction (if available = 1, if not = 0)	0,1		0	0	1	1	0	0	1
• Permanent injunction (if available = 1, if not = 0)	0,1		1	1	1	1	1	1	1
• Injunction to eliminate wrongful head start (if available = 1, if not = 0)	0,1		0	1	1	1	1	1	1
• Delivery or destruction of infringing materials (if available = 1, if not = 0)	0,1		1	1	1	1	1	1	1
• Compensatory damages (direct or out of pocket damages or consideration of profits or other damages= 1)	0,1		1	1	1	1	1	1	1
• Yielding of defendant's profits (if available = 1, if not = 0)	0,1		0	1	1	1	1	1	1
• Availability of punitive or statutory damages (if available = 1, if not = 0)	0,1		0	1	0	0	0	0	1
c) Criminal remedies									
• Fines, damages or loss of assets (if not available = 0, if minimal per expert opinion= ½, if substantial = 1)	0,1		1	1	0	0	0	0	1
• Jail sentence (if available = 1, if not = 0)	0,1		1	1	0	0	1	0	1
4. Enforcement, investigation and discovery; data exclusivity	**0-6**	**0-1**	**0.55**	**0.72**	**0.80**	**0.50**	**0.58**	**0.92**	**0.94**
• Emergency search to preserve and obtain proof (unavailable=0; available but with significant restrictions= ½ (e.g., conducted solely by an official or 3rd party expert); readily available=1)	0,1		0	1	1	1	0.5	1	1
• Ex parte emergency search availability (unavailable=0, available but with significant restrictions=½, readily available=1)	0,1		0	1	1	1	0	1	1
• Pre-trial discovery (unavailable=0, documentary only or strict limitations = ½, ready availability of documentary and interrogatories = 1)	0,1		1	0	0.5	0.5	0.5	0.5	1
• Protection of confidentiality of trade secrets in litigation (none=0, partial= ½, fully available=1)	0,1		1	1	1	0.5	0.5	1	1
b) Data exclusivity									
• Drugs (years: 0=0; 0.1-3=1/3; 3.1-7.9=2/3; >8=1)	0,1		0.66	0.66	0.66	0	1	1	0.66
• Agricultural chemicals (years: 0=0, 0.1-4.9=1/3, 5-8=2/3; > 8=1)	0,1		0.66	0.66	0.66	0	1	1	1
5. System functioning and related regulation	**0-4**	**0-1**	**0.26**	**0.14**	**0.84**	**0.28**	**0.84**	**0.83**	**0.81**
• Technology transfer: registration requirement (none=1; one or more = 0)	0,1		0	0	1	0	1	1	1
• Technology transfer: substantive review or regulation (none=1; one or more = 0)	0,1		0	0	1	0	1	1	1
• Fraser Institute score for *Legal System and Security of Property Rights* (score ranging from 0 to 10, divided by 10)	0,1		0.55	0.57	0.84	0.63	0.85	0.81	0.75
• Expert characterisation of the operation of the protection in practice (NB, based on internationally recognised or peer-reviewed sources; see country charts for details) (Generally negative = 0; none = ½; generally positive = 1)	0,1		0.5	0	0.5	0.5	0.5	0.5	0.5
Index Total (Sum of the normalised scores for the 5 categories in bold)		**0-5**	**3.09**	**2.76**	**4.07**	**3.18**	**3.60**	**4.00**	**4.57**

Notes:

1. The scoring for the Trade Secrets Protection Index (TSPI) is on a scale from zero (weakest protection) to five (strongest protection). It is the sum of the normalised scores for the five TSPI components, each with a possible range from zero to one.

2. The scores for each of the five components of the TSPI are shown in bold. The score for each component is normalised to be on a scale from zero to one. In order to normalise the score for a component, the total scores for the individual elements of the component are summed up and then divided by the total number of elements for the component. The component numbers are bolded and right justified to set them apart from the scores for the underlying elements for the corresponding component.

3. The plain text lines below each component of the TSPI show the raw scores for the individual elements of the component. The scores are centred to set them apart from the normalised component scores.

4. The period of data exclusivity for agricultural chemicals in Israel has been tentatively reported by the authorities as being greater than 8 years. Subject to confirmation via a published source (pending).

Annex 2.

Detailed Overviews for the BRICS and a Sample of OECD Countries

Introduction

This Annex presents detailed, comparable descriptions of the legal regimes for the protection of trade secrets in the BRICS countries and the 11 OECD countries covered in the sample. It includes references to statutes and key court proceedings, as well as a structured characterization of the operation of the system in each country.

The country overviews are based on a standard template covering the following aspects of the protection of trade secrets:

1. Overview
2. Scope and subject matter
3. Fault
4. Remedies
5. Procedures
6. Employee-employer relations
7. Data protection and exclusivity
8. Complementary legal institutions
9. Technology transfer

The availability of reference materials on the BRICS and OECD countries facilitated the preparation of the in-depth coverage provided here. The narrative is supported by extensive references in the text and footnotes. Most of these are drawn from statutes, recognized legal references or peer-reviewed journal articles focusing on various aspects of the protection of trade secrets.

The discussion in section 8 of the template on complementary legal institutions is somewhat more general. It draws on the Fraser Institute's Index of Economic Freedom component indicator entitled "Legal System and Security of Property Rights". That indicator is based on a separate stocktaking in each country of the functioning of the legal system as a whole.[1]

[1] See Annex 1, page 3, for a discussion of this Fraser Institute indicator:[TAD/TC/WP(2013)21/ANN1/REV1].

BRICS and OECD Country Overviews

Australia

1. Overview

Australia is a common law country with a legal system and laws derived from and similar to the legal system and laws of England. Since 1968 for federal law and 1986 for state law, the Australian High Court has been the highest court of appeal in Australia. However, before that, as a member of the British Commonwealth the decisions of the Privy Council were binding. Those earlier decisions remain precedential, and in any event Australian courts frequently look to the laws of the UK (another common law nation) for guidance.

Because of this legal heritage, Australian trade secrecy law resembles UK trade secrecy law quite closely. Australian courts frequently refer to and follow leading English decisions that are discussed in this paper's summary of UK law. At the same time, the Australian law of trade secrecy includes its own well-developed body of decisions. This summary will thus necessarily refer to UK law and portions of the UK summary, but will also take care to point out where Australian law departs from or clarifies principles from UK law.

Australia protects trade secrets almost exclusively pursuant to civil law under doctrines developed as common law. There are no statutes addressing trade secrets and no directly and generally applicable provisions in criminal law. The protections that do exist are considered to be effective.

2. Scope and Subject Matter

All commercially valuable confidential information is potentially subject to trade secrecy protection. There does not appear to be a distinction between technical information (e.g. manufacturing diagrams or formulas) and non-technical business information (e.g. customer lists) under Australian law.

a. Definitions

Australian law looks to two leading English cases for the definition of the term "trade secret." In *Coco v A.N. Clark (Engineers) Ltd.*,[2] Megarry, J., stated:

> "In my judgment, three elements are normally required if, apart from contract, a case of breach of confidence is to succeed. First, the information must itself … 'have the necessary quality of confidence about it.' Secondly, that information must have been imparted in circumstances importing an obligation of confidence. Thirdly, there must be an unauthorised use of that information to the detriment of the party communicating it."

Later, in *Searle Australia Pty. Ltd. v. Public Interest Advocacy Center & Anor.*,[3] the full Australian Federal Court adopted the definition of trade secret from *Lansing Linde Ltd v Kerr*, where Staughton L.J., further elaborated:

---

2 Coco v. A.N. Clark (Engineers) Ltd. [1969] RPC 41. Followed by numerous Australian courts, including Moorgate Tobacco Co. Ltd. v. Philip Morris Ltd. (No. 2) (1984) 156 CLR 414; Mainbridge Industries Pty. Ltd. v. Whitewood (1984) 73 FLR 117.

3 Searle Australia Pty. Ltd. v. Public Interest Advocacy Center & Anor (1992) 36 FCR 111.

> ‘‘What are trade secrets, and how do they differ (if at all) from confidential information? ... I would add first, that it must be information used in a trade or business, and secondly that the owner must limit the dissemination of it or at least not encourage or permit widespread publication.’’

In sum, in Australia, a trade secret is information that:

(1) Is used in business;

(2) Has a confidential quality, and the owner has attempted to limit dissemination;

(3) Was disclosed to the defendant under confidential circumstances; and

(4) Defendant has used or disclosed the information (or threatens to do so) to the detriment of the owner.

b. Scope and Subject Matter Under Civil Law

- ***Used in Business.*** Under Australian law, “it is not the type or nature of the information that of itself determines whether protection will be provided by the courts in any particular case.”[4] Notably, the Australian courts have rejected[5] the distinction made in the English case of *Faccenda Chicken Ltd. v. Fowler*,[6] between business information and “secret processes of manufacture,” following instead[7] a later leading case, *Lansing Linde Ltd v Kerr*,[8] which takes a broader view of trade secret protection. A leading treatise[9] compiled the following list of examples from Australian case law, which demonstrates the breadth of business information covered by Australian law:

  – data detailing impurities, analytical tests, stability and bio-availability regarding a therapeutic substance documents relating to the importation of a drug

  – data concerning the efficacy and effects of contraceptive devices and tests undertaken on or in relation to them

  – customer history cards and artwork relating to the printing of customized business forms and stationery

  – details of the on-going fit-out of premises for a credit union, including budget, customer requirements and timing

  – information regarding an Australian patent application that was not yet in the public domain

  – a proposal for a survey of law firms and a draft questionnaire

4 Terrence MacLaren, Trade Secrets Throughout the Word, § 2.3 (2012) (citing cases) (hereinafter MacLaren, Trade Secrets Throughout the Word).

5 Wright v. Gasweld Pty. Ltd. (1991) 22 NSWLR 317 at 335, 339.

6 [1986] 1 All ER 617.

7 Searle Australia Pty. Ltd. v. Public Interest Advocacy Center & Anor (1992) 36 FCR 111.

8 [1991] 1 W.L.R. 251.

9 The list is quoted in its entirety from MacLaren, Trade Secrets Throughout the World § 2.3.

- a report on tests of lubricating oil
- the identity of an informant
- information concerning reliable agents and manufacturers in Chinese Taipei
- budwood cuttings for nectarine trees
- the idea for use of a pressure control valve in hydraulically operated gymnasium equipment
- information regarding the design, construction and operation of a rubber glove machine
- the specifications and tolerances of a friction bolt

- ***Confidential Quality.*** The information that is the subject of trade secrecy must not be in the public domain. Secrecy need not be absolute, but dissemination must be limited to parties with some obligation to keep the information secret.[10] Once information enters the public domain, at least through the fault of plaintiff, it generally ceases to be confidential.[11] Courts will consider the extent of the measures taken by plaintiff to secure the information, as well as how widely it is known within and outside of the business.[12]

- ***Disclosed to the Defendant Under Confidential Circumstances.*** The Australian courts cite the requirement from *Coco v. A.N. Clark*[13] and other English cases that the information must be communicated under conditions that create an obligation of confidentiality. As discussed in this paper's summary of UK law, this requirement may suppose that there must be some relationship between the parties, but, as also discussed, UK law appears to have evolved away from this requirement. Australian law is clearer on this point. According to *Moorgate Tobacco Co. Ltd. v. Philip Morris Ltd.*, trade secret protection "lies in the notion of an obligation of conscience arising from the circumstances in or through which the information was communicated or *obtained*."[14] (emphasis added). Courts will thus look to whether the information was surreptitiously obtained as well as whether it was communicated in confidence.[15] Thus, in *Franklin v. Giddins*,[16] the theft of cuttings from a new variety of nectarine by a trespassing neighbour was treated as trade secret theft. As the judge said in refusing to limit trade secret protection to instances where the parties had a relationship, "I find myself quite unable to accept that a thief who steals a trade secret, knowing it to be a trade secret, with the intention of using it in commercial competition with its owner, to the detriment of the latter, and so uses it, is less conscionable than a traitorous

10 Coco v. A.N. Clark Eng'rs Ltd., [1969] RPC 41; Wright v. Gasweld Pty. Ltd. (1991) 22 NSWLR 317.

11 Australian Broadcasting Corporation v. Lenah Game Meats Pty Ltd (2001) 54 IPR 161.

12 Wright v. Gasweld Pty. Ltd. (1991) 22 NSWLR 317.

13 Coco v. A.N. Clark Eng'rs Ltd., [1969] RPC 41; Wright v. Gasweld Pty. Ltd. (1991) 22 NSWLR 317.

14 Moorgate Tobacco Co. Ltd. v. Philip Morris Ltd. (No. 2) (1984) 156 CLR 414 at 438.

15 Commonwealth v. John Fairfax & Sons Ltd. (1980) 147 CLR 39.

16 Franklin v. Giddins [1978] Qd R 72, 80.

servant."[17] Of course, regardless of how the information is obtained or communicated, it must meet the requirement of confidentiality described above.

- ***Use or disclosure of information to the detriment of the owner.*** It may be necessary for the owner to show that use or disclosure is likely to harm him, at least in order to receive an injunction.[18] In most instances such harm is likely to be present, but the requirement might prove problematic for a party that owns but does not use or intend to use information. (For example, information about the second-best way to manufacture a product, where the owner is already using the best method.) "The question as to whether detriment needs to be shown is open in Australia, [but] in any event, apprehended prejudice such as would be relevant to the granting of [preliminary, anticipatory] relief is likely to be sufficient detriment."[19]

c. Scope and Subject Matter Under Criminal Law

Australia's criminal law does not protect trade secrets. There are instances where a crime committed in the course of appropriating a trade secret might be punished. These instances include burglary, intercepting communication, unauthorized access to a computer, or conspiracy to defraud.[20] However, the underlying information is not protected as a trade secret.

3. Fault

a. Standard Under Civil Law

Civil trade secrecy law in Australia does not frame the cause of action for trade secret in terms of fault, such as through intentional or negligent disclosure. Rather, as discussed earlier, the offense is in using or disclosing the information in breach of a duty not to do so, regardless of whether the using or disclosing party intends to breach the duty or harm the claimant. In contrast to UK law, however, it is clear that a defendant who knowingly appropriates confidential information through eavesdropping, theft or other wrongful act will be treated as having a constructive obligation not to reveal the information. For example, in *Franklin v. Giddins*,[21] the court treated defendant, a neighbour who had trespassed to steal confidential material as a "constructive trustee" with the same obligations of an agent of the plaintiff.

Innocent third parties are most likely not excused from liability. In *Wheatley v. Bell*[22] the Supreme Court of New South Wales rejected the applicability of the concept of a bona fide purchaser for value. In that case, the court enjoined defendant's innocent franchisees.

b. Criminal Law

The issue of fault in criminal trade secrecy is irrelevant in Australia, due to lack of a criminal statute.

---

17 Ibid. at 80.

18 Coco v. A.N. Clark Eng'rs Ltd., [1969] RPC 41.

19 MacLaren, Trade Secrets Throughout the Word, § 2.7 (2012).

20 MacLaren, Trade Secrets Throughout the Word, § 2.4 (2012).

21 Franklin v. Giddins, [1978] Qd R 72, 81.

22 Wheatley v. Bell [1982] 2 NSWLR 544.

4. Remedies

a. Civil Law

The following remedies are available:

- Injunctive relief, both interlocutory and permanent.[23]
- Seizure and destruction of infringing materials pursuant to an order for delivery up.[24]
- Monetary relief, either in the form of compensatory damages or recovery of defendant's profits.[25] Exemplary damages are available in theory, but have not yet been applied in practice.[26]

Injunctive relief is not mandatory. If a defendant's actions effectively make the information public, then the information may no longer be confidential, thus precluding an injunction,[27] but not monetary remedies. Even where information has become public, a defendant may be enjoined for a limited period to negate its improper "head start" in obtaining the information.[28]

b. Criminal Law.

Not applicable.

5. Procedures

a. Emergency Action to Preserve Proof

In Australia, as in the UK, an ex parte procedure known as an Anton Piller Order is potentially available to plaintiffs seeking to preserve proof. The procedure allows the plaintiff to apply directly to the court without informing the potential defendant. If granted, the plaintiff may search the defendant's premises and seize documents. The order allowing this procedure may be no more broad than is necessary to preserve the relevant evidence. An Anton Piller Order is granted at the discretion of the court upon a showing that it is necessary to preserve evidence.

As discussed in this paper's summary of UK law, Anton Piller orders have proven to be controversial in some cases. In response to criticism of the orders, the Chief Justice of the Australian Federal Court issued "Federal Court Practice Note No. 24—Search Orders (also known as "Anton Piller Orders")."[29] The Practice Note regulates Anton Piller orders to ensure they do not violate parties' rights and that they are not granted as a matter of routine, but rather must be fully justified by an extremely strong prima facie case and a need to preserve evidence from a real possibility of destruction or concealment.

---

23 Australian Broadcasting Corporation v. O'Neill, [2006] HCA 46; 80 ALJR 1672.

24 MacLaren, Trade Secrets Throughout the Word, § 2.18 (2012).

25 MacLaren, Trade Secrets Throughout the Word, § 2.19 – 2.20 (2012).

26 MacLaren, Trade Secrets Throughout the Word, § 2.19 – 2.20 (2012).

27 Attorney General v. Guardian Newspapers Ltd. (No. 2), [1988] 3 All ER 545. (Lord Donaldson, M.R.).

28 British Franco Electric Pty. Ltd. v. Dowling Plastics Pty. Ltd. [1981] 1 NSWLR 448.

29 Federal Court Practice Note No. 24—Search Orders (also known as "Anton Piller Orders") (5 May 2006).

A further preliminary procedure is available in Federal Court under Order 15A.[30] This Order allows discovery before a proceeding is commenced in order to obtain the identity of the defendant or determine whether to commence a proceeding. The court may allow inspection of documents and material evidence as well as examination of witnesses.

b. Pre-Trial Discovery

In Australia, pre-trial discovery is available but generally limited to documentary evidence.

c. Secrecy During Litigation

In Australia, procedures safeguard the secrecy of plaintiff's confidential information during trade secret litigation. The plaintiff can obtain closed or "in camera" hearings for both pre-trial procedures and the trial.[31]

6. Employee-Employer Relationships

Australian law enforces both implied and express duties imposed on employees to keep information confidential, but is also protective of employee's ability to earn a living after leaving an employer. Australian courts will enforce express contractual duties to keep information confidential, both during and after employment. Unlike UK law, Australian law does not distinguish between the duties of current and former employees with respect to the *types* of confidential information protectable pursuant to an agreement.[32] It will also imply a duty to keep an employer's confidential information secret.

Australian courts, however, are reluctant to enforce either trade secret agreements or covenants not to compete if they affect an employee's ability to earn a living.[33] A guiding consideration is to allow former employees to exercise skills and general knowledge so as not to impede employment prospects. Moreover, duties will not be enforced unless they are reasonable with respect to time and geographic scope.

Australian courts will also enforce implied duties of confidentiality. Such duties are broad during employment. After employment, they include specific trade secrets, but not know how that has become part of the employees' skills and general knowledge.[34]

7. Data Exclusivity and Data Protection

Australia provides the following data exclusivity protection: (a) 5 years for drugs with new active components; and (b) 11 years for agricultural and veterinary products with new active ingredients.[35] During the period of exclusivity, which begins on the date of registration, no other party may receive the registrant's data nor may they rely on it for an application to register an equivalent product.

---

30 Order 15A of the Rules of the Federal Court.

31 H.P. Lee & Enid Campbell, The Australian Judiciary 63-64 (2d ed. 2013).

32 Wright v. Gasweld Pty. Ltd. (1991) 22 NSWLR 317 at 335, 339.

33 Ansell Rubber Co. Pty. Ltd. v. Allied Rubber Industries Pty. Ltd. [1967] VR 37.

34 Ibid; MacLaren, Trade Secrets Throughout the Word, § 2.11 (2012).

35 Therapeutic Goods Act 1989; Agricultural and Veterinary Chemicals Code Act 1994.

With respect to drugs, "data exclusivity is not provided for new dosage forms, routes of administration, indications or combinations with other active ingredients."[36] To be a "new" chemical entity, the ingredient must have never been registered before in any form.[37]

With respect to agricultural and veterinary products, the exclusivity period is 5 years if the same data is used to register another *agricultural* product or to change labelling, or 3 years if the same data is used to register another *veterinary* product or to change labelling.[38]

8. Complementary Legal Institutions

Australia's commercial legal system is well regarded. On the 2012 Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, Australia receives a score of 8.1 out of 10, which ranks it 13th in the world.[39]

9. Technology Transfer

Australia does not subject foreign investors to technology transfer requirements, joint venture technology contribution requirements, or license registration requirements.

36 Joanna Jones, Data exclusivity provisions under the Therapeutic Goods Act 1989, http://www.davies.com.au/pub/detail/234/data-exclusivity-provisions-under-the-therapeutic-goods-act-1989 (August 2009).

37 Alphapharm Pty Ltd v H Lundbeck A/S [2008] FCA 559.

38 Joanna Jones, Data exclusivity provisions under the Therapeutic Goods Act 1989, http://www.davies.com.au/pub/detail/234/data-exclusivity-provisions-under-the-therapeutic-goods-act-1989 (August 2009).

39 Fraser Institute, Economic Freedom of the World 2012 Annual Report at 33 (2012).

Brazil

1. Overview

Brazil has enacted protection for trade secrets, although the efficacy of the laws on the books is limited somewhat by certain practical difficulties in establishing and protecting trade secrets. In general, "[b]ecause few cases have been tested in court, Brazil lacks a substantial jurisprudence on trade secrets."[40] Experts describe court rulings on key issues as "few" or "scanty."[41] More specifically, a number of policies and legal provisions tend to counteract the strength of otherwise broad trade secret protection.

As described further below, Brazil's protection for trade secrets is generally strong with respect to definition and scope, but certain limitations on licensing limit the effective scope of trade secret protection. The law lacks a precise definition of trade secrets, but experts observe that Brazilian law treats trade secrets in a manner typical of international norms, covering both commercial and technical information. The law provides for both civil and criminal sanctions. In Brazil, a private party may initiate a criminal trade secret suit and may also pursue civil remedies. Thus, the process for seeking a remedy for trade secret infringement may encompass a criminal and civil proceeding, with all remedies from both kinds of actions available. The law sanctions both misappropriation and breach of duty.

On the other hand, Brazil places extraordinary restrictions on commercial agreements involving trade secrets. The Brazilian Patent and Trademark Office's ("BPTO") has a role in approving license agreements for intellectual property. As discussed in detail below, the BPTO disapproves of trade secret licenses, and places strict limits on important aspects of such licenses. This disapproval represents a major challenge for effectively enforcing trade secrets in Brazil and entering effective agreements with other businesses concerning trade secrets. Effectively, the scope of trade secret protection in Brazil is significantly limited by this restriction. A trade secret owner can protect the trade secrets against commercial espionage and breach of duty by employees and business partners, but Brazilian law limits the owner's ability to engage in the very common practice of licensing and to protect secrets in that context. This restriction severely limits the effectiveness of trade secret protection in Brazil.

In addition, commentators and experts have observed that a number of other provisions make trade secret protection less effective. For example, criminal penalties are relatively low:

> Violation of trade secrets (and of Industrial Property rights in general) is treated by our statutory law as a "crime of lower offensive potential". Penalties foreseen are low ("detention of 3 (three) months to 1 (one) year) or a fine") and their lack of effectiveness together with the difficulties to recover damages create relative values and enforcement difficulties.[42]

---

40 MacLaren, Trade Secrets Throughout the World § 5:8 (2012).

41 MacLaren, Trade Secrets Throughout the World § 5:3 – 5:4 (2012).

42 Elisabeth K. Fekete, et al., AIPPI Report Q215, Protection of Trade Secrets Through IP and Unfair Competition Law, Brazil 7 (2010).

One expert report notes several issues with Brazilian trade secret law.[43] Particularly notable is the difficulty in obtaining injunctions:

> 1) First: As mentioned …, the contractual aspects regarding trade secrets may be considered a very important issue for Brazil. BPTO's interpretation that trade secrets cannot be licensed creates practical limitations (i.e. for the contract drafting and, subsequently, for the ability of the holder to control its use) when the agreements are subject to registration before such office. Court decisions from the eighties (80's) accepted BPTO's unlimited competence for this interpretation. Currently, certain sparse decisions criticizing BPTO's policies when registering agreements were rendered, but one cannot yet assert that there is a final/definite case law orientation about this issue or even that there is a significant volume of precedents. Therefore, it is needed for improvement of the Brazilian system that a clear definition be adopted by the Courts on the possibility of trade secret to be licensed in Brazil and, eventually, new policies or interpretations of the BPTO be adopted accepting this position, or at least formulating an official guideline on its policies on this subject, to be used by contractual parties.
>
> 2) Second: Violation of trade secrets (and of Industrial Property rights in general) is treated by our statutory law as a "crime of lower offensive potential". Penalties foreseen are low ("detention of 3 (three) months to 1 (one) year) or a fine") and their lack of effectiveness together with the difficulties to recover damages create relative values and enforcement difficulties.
>
> 3) Third: Although injunctions are rendered, the slowness of our Judiciary system is often incompatible with trade secret dynamics.
>
> 4) Fourth: Trade secret protection has evolved and improved in our country, but there is less awareness of its protection in the public sector and one still sometimes finds judges that require the presentation of the "registration" of the secret.
>
> 5) Fifth: Experts' reports and evidence in general are often difficult obstacles to overcome in trade secret litigation and deserve more study and development.
>
> 6) Sixth: Improvements for the protection of trade secrets during litigation are desired.
>
> 7) Seventh: Our Customs authorities are not prepared nor equipped to evaluate trade secrets violations in case of necessity to apply retention measures … .

Furthermore, Brazil essentially does not protect data submitted for regulatory approval of pharmaceuticals. The pharmaceutical industry in the U.S. has criticized this policy, as discussed further below.

2. Scope and Subject Matter

a. Definitions

Brazilian law lacks a specific definition of trade secret, but contains sufficient content to supply an implicit one. For example, Art. 195, Sections XI – XII state that an individual commits an offense of unfair competition if he:

[43] Elisabeth K. Fekete, et al., AIPPI Report Q215, Protection of Trade Secrets Through IP and Unfair Competition Law, Brazil 9 - 10 (2010).

> XI. 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;
>
> XII. divulges, exploits or utilizes, without authorization, the kind of knowledge or information to which the previous Item refers, when obtained by illicit means or when access was gained through fraud.[44]

Although this statutory section does not explicitly define trade secrecy, it provides an implicit definition. Trade secrets are commercially valuable information ("confidential knowledge, information or data that could be used in industry, commerce or rendering of services") that is actually kept secret ("confidential" and not information "that would be evident to a technician versed in the subject").

Expert commentary confirms this implicit reading drawn from the statute. As one expert observes, the statutes supplies a basis, and "[m]ore detailed principles are supplied by case law and court precedents, being also the relevant provisions of the TRIPS Agreement directly applicable to this specific matter."[45] This expert thus defines trade secrecy in Brazil as follows:

> A definition in Brazil can be based on the conditions required by Art. 39.2 of TRIPS, complemented by the features that are considered reasonable for enforcement purposes in our country and that are expressly foreseen or implicit in Art. 195, subsections XI and XII of BIPL: "A trade secret is confidential knowledge, information or data, usable in industry, commerce or services, that is lawful, transmissible, has economic value and is subject to reasonable steps to be kept secret and that is not of public knowledge or obvious to a person skilled in the art". In our jurisdiction, we believe it is possible to adopt, for discussion purposes, a definition of trade secrets like the one of the previous paragraph, based on the applicable statutory law ... .[46]

The statutory provisions from the 1996 Industrial Property Law discussed above establish criminal offenses, but they also serve as the basis for defining trade secrets under criminal law. As one commentator explains, "civil damages can also be sought in a related civil suit, not only on the grounds of the general rule that a crime may also involve a civil wrong, but also on the grounds of a special provision inserted into Article 206 of the 1996 Industrial Property Law which expressly contemplates the possibility that the injured party may claim civil damages arising out of the criminal act."[47]

Thus, requirements common to many countries are applicable in Brazil: the information must be commercial information, broadly understood; it must actually be secret; and the owner must take reasonable steps to safeguard secrecy.

---

44 Law No. 9.279 of May 14, 1996 (Industrial Property Law), Art. 195, Sections XI – XII, unofficial translation available at http://www.wipo.int/wipolex/en/text.jsp?file_id=125397.

45 Elisabeth K. Fekete, et al., AIPPI Report Q215, Protection of Trade Secrets Through IP and Unfair Competition Law, Brazil 4(2010).

46 Elisabeth K. Fekete, et al., AIPPI Report Q215, Protection of Trade Secrets Through IP and Unfair Competition Law, Brazil 1 - 2 (2010).

47 MacLaren, Trade Secrets Throughout the World § 5:9 (2012).

b. Scope and Subject Matter Under Civil Law

The subject matter of trade secret protection in Brazil is apparently broad, but effectively limited by technology transfer regulations. As described above, the Industrial Property Law protects "confidential knowledge, information or data that could be used in industry, commerce or rendering of services."[48] This language appears to cover technical information and confidential business information, as well as know-how. Expert commentary confirms this broad coverage, based on the "few holdings of Brazilian courts on this matter"[49] or "scanty jurisprudence."[50]

As described further below, however, trade secrets are not effectively protectable in the context of commercial business relationships because the Brazilian Patent and Trademark Office disapproves of them and strictly limits protection of them. This regulation limits the scope of trade secret protection, making it effective with respect to employees, fiduciaries, and some third parties, but nullifying it in the context of common commercial relationships.

c. Scope and Subject Matter Under Criminal Law

The scope and subject matter of criminal sanctions for trade secret behavior is generally the same as with respect to civil protection. Both technical information and confidential business information are protected.

3. Fault

a. Standard Under Civil Law

Brazilian trade secret law prohibits both misappropriation of trade secrets and the misuse or wrongful disclosure of trade secrets in breach of duty. Article 195, Section XII covers misappropriation, as it prohibits unauthorized disclosure, use, or exploitation of trade secrets when the information was "obtained by illicit means or when access was gained through fraud."[51] Article 195, Section XI covers breach of duty, as it prohibits unauthorized disclosure, use, or exploitation of trade secrets "to which [one] gained access by means of a contractual or employment relationship, even after the termination of the contract."[52]

The concept of misappropriation does not appear to be defined in complete detail in Brazil. It covers "illicit means" and fraud, which would appear to include crimes, torts, and other clearly wrongful acts. What is not clear is whether the more opportunistic forms of industrial espionage that do not constitute torts or crimes are covered – for example, going to extraordinary lengths to eavesdrop on or photograph a competitor's premises without actually trespassing or committing another act that is in and of itself wrongful. The available commentaries are silent on this point, but as discussed above, they do note that the precedents

48 Law No. 9.279 of 14 May 1996 (Industrial Property Law), Art. 195, Section XI, unofficial translation available at http://www.wipo.int/wipolex/en/text.jsp?file_id=125397.

49 MacLaren, Trade Secrets Throughout the World § 5:3 (2012).

50 MacLaren, Trade Secrets Throughout the World § 5:4 (2012).

51 Law No. 9.279 of May 14, 1996 (Industrial Property Law), Art. 195, Section XII, unofficial translation available at http://www.wipo.int/wipolex/en/text.jsp?file_id=125397.

52 Law No. 9.279 of May 14, 1996 (Industrial Property Law), Art. 195, Section XI, unofficial translation available at http://www.wipo.int/wipolex/en/text.jsp?file_id=125397.

are few. However, one expert has observed that industrial and commercial espionage are covered by Brazilian law.[53]

Breach of duty is better defined under Brazilian law. As the statutory language observes, a "contractual or employment relationship" will give rise to a duty not to disclose, use, or exploit a trade secret. Both employees and fiduciaries have an implicit duty not to disclose, regardless of whether any explicit contract exists.[54] (But see the discussion below of the BPTO's regulation of trade secret licenses, which interferes with imposing a duty in the context of many common commercial relationships.)

Third parties also may be liable for using or disclosing trade secrets if they have knowledge that the trade secret was disclosed in breach of duty or otherwise misappropriated.[55] However, an innocent third party is unlikely to be held liable.[56] As for a party who has reason to know they have received a trade secret that was obtained in violation of law, the standard likely is gross negligence:

> Although no case law is known in this issue, Brazilian courts would probably apply the concept of "grossly negligent" third parties referred to in footnote 102 of Article 39,2 of TRIPS in the following: business men are supposed to know or to take the necessary precautions within their companies to be aware of which information is or has a potential to be a trade secret, under reasonable situations.[57]

Thus, the law prohibits (1) misappropriation of a trade secret; (2) unauthorized use or disclosure in breach of a contractual or other duty; or (3) receipt of the trade secret with knowledge or reason to know that it was in violation of the latter two prohibitions.

b. Standard Under Criminal Law

The type of offenses covered by criminal sanctions for trade secret theft in Brazil is essentially the same as with respect to civil protection. In fact, as noted above, the standards derive from the criminal provisions in the Industrial Property Act.

4. Remedies

a. Remedies Under Civil Law

Brazilian law provides a wide array of remedies. These remedies are available:

---

53 Elisabeth K. Fekete et al., AIPPI Report Q215, Protection of Trade Secrets Through IP and Unfair Competition Law, Brazil 4 (2010). The report was commenting affirmatively on whether Brazilian law prohibited acts covered by a resolution passed by the NGO AIPPI, the Q115 Copenhagen Resolution, which urged that national trade secret laws prohibit "industrial or commercial espionage." AIPPI, Resolution on Question 115 Effective protection against unfair competition under Article 10bis Paris Convention of 1883 (1994), available at https://www.aippi.org/download/commitees/115/RS115English.pdf.

54 MacLaren, Trade Secrets Throughout the World § 5:11 (2012).

55 Elisabeth K. Fekete et al., AIPPI Report Q215, Protection of Trade Secrets Through IP and Unfair Competition Law, Brazil 5 (2010).

56 Ibid.

57 Ibid.

- Both preliminary and permanent injunctions;[58]
- Compensatory damages, including lost profits;[59]
- Alternately, damages may be based on defendant's profits or the license fee that defendant would have paid to the plaintiff;[60]
- Seizure and eventual destruction of infringing goods.[61]

Ex parte injunctions in the form of temporary restraining orders are available.[62] One expert noted that "[a]lthough the violation of trade secrets is theoretically subject to punitive damages, we do not know of any case law in this concern."[63]

b. Remedies Under Criminal Law

Trade secret infringement is treated as a "crime of lower offensive potential" in Brazil, which, experts note, leads to relatively low punishment and limited effectiveness.[64] Criminal sanctions are imposed on individuals only, with prison sentences three months to a year.[65] The amount of fines is unspecified, but likely to be low given the low-priority status of trade secret infringement as a crime.[66]

5. Procedures

a. Emergency Action to Preserve Proof

Preliminary search and seizure actions to collect evidence are available under both the criminal and civil laws.[67] Such orders are "subject to evidence being presented to the court that the plaintiff has a clear right and that the defendant's actions would otherwise cause irreparable injury."[68]

58 MacLaren, Trade Secrets Throughout the World, § 5:13 (2012); Elisabeth K. Fekete, et al., AIPPI Report Q215, Protection of Trade Secrets Through IP and Unfair Competition Law, Brazil 4 - 5 (2010).

59 MacLaren, Trade Secrets Throughout the World, § 5:13 (2012); Elisabeth K. Fekete, et al., AIPPI Report Q215, Protection of Trade Secrets Through IP and Unfair Competition Law, Brazil 4 - 5 (2010).

60 MacLaren, Trade Secrets Throughout the World, § 5:13 (2012); Elisabeth K. Fekete, et al., AIPPI Report Q215, Protection of Trade Secrets Through IP and Unfair Competition Law, Brazil 4 - 5 (2010).

61 MacLaren, Trade Secrets Throughout the World, § 5:13 (2012); Elisabeth K. Fekete, et al., AIPPI Report Q215, Protection of Trade Secrets Through IP and Unfair Competition Law, Brazil 4 - 5 (2010).

62 MacLaren, Trade Secrets Throughout the World, § 5:13 (2012); Elisabeth K. Fekete, et al., AIPPI Report Q215, Protection of Trade Secrets Through IP and Unfair Competition Law, Brazil 4 - 5 (2010).

63 Elisabeth K. Fekete, et al., AIPPI Report Q215, Protection of Trade Secrets Through IP and Unfair Competition Law, Brazil 4 - 5 (2010).

64 Elisabeth K. Fekete, et al., AIPPI Report Q215, Protection of Trade Secrets Through IP and Unfair Competition Law, Brazil 10 (2010).

65 Ibid.

66 See ibid.

67 Ibid at 4 citing Articles 273 and 461 of the Code of Civil Procedure and Article 525 of the Code of Criminal Procedure.

68 MacLaren, Trade Secrets Throughout the World § 5:13 (2012).

b. Pre-Trial Disclosure and Discovery

Pre-trial discovery in Brazil is limited and is largely documentary, conducted under the supervision of the judge.[69] "The concept of party-initiated pre-trial discovery does not exist in Brazil. Moreover, the parties may not compel one another to produce evidence without the participation of the court."[70]

c. Secrecy During Litigation

Brazilian law establishes the right of parties in litigation to have trade secrets reviewed in camera and otherwise protected from misuse by the other party.[71] Parties can also request the court to provide special security for physical evidence.[72]

6. Employee-Employer Relationships

Both express and implied obligations to protect trade secrets are enforceable against current and former employees and business partners.[73] Post-relationship express and implied duties are also generally enforceable.[74] However, there is a major caveat to this point: technology transfer regulations governing licenses prohibit limiting use of information after expiration of agreement, and the term of such agreements is limited to 19 years.[75] Thus, commercial agreements between companies can provide only limited protection for trade secrets.

Non-competition provisions may be struck from an agreement by administrative authorities or courts if viewed as a violation of competition law.[76] They must be related to the protection of trade secrets and be limited in duration and geographic scope.[77] In employment agreements, they must provide remuneration to the former employee, paying them a stipend for the duration of the non-compete period.[78]

7. Data Protection and Exclusivity

Brazil does not provide protection for information submitted for regulatory approval of pharmaceuticals, but does do so for agricultural products and veterinary drugs. The Brazilian Pharmaceutical Regulatory Agency may approve a generic drug application based on prior

69 Carlos Roberto Siqueira Castro, et al., Latin Lawyer: Litigation 2013 (2012), available at http://latinlawyer.com/reference/topics/60/jurisdictions/6/brazil/; Fernando Eduardo Serec, International Civil Procedure: Brazil § 5.2 (2003).

70 Fernando Eduardo Serec, International Civil Procedure: Brazil § 5.2 (2003).

71 Elisabeth K. Fekete, et al., AIPPI Report Q215, Protection of Trade Secrets Through IP and Unfair Competition Law, Brazil 6 (2010) (citing Article 206 of the Industrial Property Law).

72 Elisabeth K. Fekete, et al., AIPPI Report Q215, Protection of Trade Secrets Through IP and Unfair Competition Law, Brazil 6 (2010).

73 MacLaren, Trade Secrets Throughout the World § 5:11 (2012).

74 MacLaren, Trade Secrets Throughout the World § 5:11 (2012); Elisabeth K. Fekete, et al., AIPPI Report Q215, Protection of Trade Secrets Through IP and Unfair Competition Law, Brazil 8 (2010).

75 MacLaren, Trade Secrets Throughout the World § 5:14 (2012).

76 MacLaren, Trade Secrets Throughout the World § 5:12 (2012).

77 Ibid.

78 Ibid.

approval of a new chemical entity at any time.[79] Brazil does provide data protection of 10 years for agricultural products and veterinary drugs for new chemical entities and 5 years for new uses and indications.[80]

This lack of protection for pharmaceuticals has been heavily criticized by foreign pharmaceutical companies. The U.S. trade group, PhRMA, submitted these comments in the US Special 301 process:

> The Brazilian Government still adopts a flexible interpretation of Article 39 of the TRIPS Agreement to allow Government officials to grant marketing approval relying on test and other data submitted by our member companies to prove the safety and efficacy of their products. While some positive steps have been taken to prevent inappropriate disclosure of these data held by the Government, additional efforts are needed to provide certainty that test and other data will be protected fully against unauthorized use to secure marketing approval for a fixed period of time. Our member companies continue efforts to gain protection for their data through the Judiciary System, with limited success. The intense debate in the Judiciary demonstrates the lack of clarity in the Brazilian legal framework regarding RDP protection for pharmaceuticals. Although federal law 10.603/02 provides adequate protection for veterinary and crop products, the Brazilian legislation still does not provide a similar benefit for pharmaceutical products, resulting in discriminatory treatment. A productive dialogue among U.S. and Brazilian authorities could lead to an appropriate RDP regime for pharmaceutical products in Brazil by assuring that the domestic legislation meets high standards. In conclusion, Brazil lacks sufficient protection for data submitted for innovative biopharmaceutical products. A period of data protection preventing ANVISA from relying on the innovator's data in approving a follow-on medicine application is needed. Although there have been lawsuits seeking to secure a period of data protection for specific products, so far the Courts are split, leaving innovators without reliable regulatory data protection.[81]

8. Complementary Legal Institutions

On the Fraser Institute *Index of Economic Freedom*'s component index for Legal System and Security of Property Rights, Brazil receives a score of 5.24 out of 10, which ranks it 77th in the world.[82] Its lowest scores are with respect to integrity of the legal system (3.33 out of 10) and reliability of police (3.97 out of 10).[83]

9. Technology Transfer

Brazil maintains some of the world's most extensive technology transfer regulations affecting trade secret licensing. As one expert report observes, "the regulation on restrictive

---

79 Gabriel Di Blasi, Data Exclusivity Protection in Brazil, World Intellectual Property Review 32 (November/December 2009), available at http://www.pedrofolio.com/clientes/diblasi/arquivos_pdf/724.pdf.

80 Ibid.

81 PhRMA Special 301 Submission 2013 at 85 – 86, available at: http://www.phrma.org/sites/default/files/pdf/PhRMA%20Special%20301%20Submission%202013.pdf.

82 Fraser Institute, Economic Freedom of the World 2012 Annual Report at 46 (2012).

83 Ibid.

business practices [such as limited licenses] has not yet evolved from a centralized and technology transfer-oriented focus to a merely market-oriented one."[84]

Agreements for licensing intellectual property must be registered with and authorized by the Brazilian Patent and Trade Mark Office (BPTO) "for three purposes . . . (i) authorization of remittance of payments abroad; (ii) income tax deduction benefit and (iii) enforceability before third parties."[85] Essentially, thus, all license agreements of consequence must be subject to regulation and approval by the BPTO. The BPTO disfavors licensing of non-patented technology[86] (i.e., trade secrets), and there are particular clauses the BPTO will not approve. One expert observed the following practices:

> [T]he Brazilian Patent and Trademark Office (BPTO), ... does not authorize clauses (i) limiting the use of the know-how, even after the termination of the agreement, (ii) of unlimited confidentiality term, and (iii) requesting devolution of materials from the licensor, for example. The interpretation of the BPTO is that technology not protected by a patent can only be "transferred" to a Brazilian party rather than "licensed", therefore, the trade secret may be assigned ('sold'), but not "licensed".[87]

It thus appears that a trade secret cannot be licensed, rather than transferred.

Other commentary notes that, the following provisions are prohibited:[88] (1) limiting use of information after expiration of agreement; (2) requiring return of materials (e.g. documents) at the termination of the agreement; and (3) providing an unlimited term (terms are typically limited to 19 years at the most).

In sum then, trade secret protection in Brazil is very limited in the context of foreign direct investment, joint ventures, franchising, distribution, manufacturing agreements, outsourcing, and other common commercial agreements where one party licenses a trade secret to another.

84 Elisabeth K. Fekete, et al., AIPPI Report Q215, Protection of Trade Secrets Through IP and Unfair Competition Law, Brazil 7 (2010).

85 Ibid.

86 MacLaren, Trade Secrets Throughout the World § 5:14 (2012).

87 Elisabeth K. Fekete, et al., AIPPI Report Q215, Protection of Trade Secrets Through IP and Unfair Competition Law, Brazil 7 (2010).

88 MacLaren, Trade Secrets Throughout the World § 5:14 (2012).

China

1. Overview

Chinese law contains comprehensive civil, criminal and administrative protections for trade secrets. While the laws on the books are strong and effective in many respects, their efficacy is severely undermined by certain key aspects of the law, particularly evidentiary requirements, procedures, and practices. These limitations make preliminary injunctions exceedingly rare and make it difficult to prove the existence of trade secrets. These shortcomings motivate experts to urge trade secret owners into a de facto set of formalities for trade secrets – that they be subject to agreements, specifically described in writing, and acknowledged by the recipient – in order to make rights enforceable. In addition, businesses appear to have poor perceptions of trade secret protection in China, and foreign governments have identified a serious and persistent threat of organized industrial espionage originating in China.

Comments from the business sector reflect poor perceptions regarding how well China protects trade secrets within China. In 2009, the security firm McAfee surveyed "1 000 senior IT decision makers in the US, UK, Japan, China, India, Brazil and the Middle East."[89] The report found that about 50% of respondents rated the "threat level" to their sensitive data in China as "high."[90] The report related the following perceptions:

> Three countries, in particular, stood out to the survey respondents—perhaps reflecting broader security perceptions. Respondents cited China, Pakistan and Russia as the worst-rated countries when it comes to the protection of digital assets. Pakistan, China and Russia, in that order, were also perceived to have the worst reputations for pursuing or investigating security incidents. Respondents cited corruption among law enforcement and the legal systems as well as poor skills among law enforcement as top reasons for the reputation rating.[91]

The report also found that over 25% of respondents had avoided doing business in China due to security concerns.[92] A 2011 survey of international business executives by McAfee and SAIC found these concerns about China unabated, as survey respondents once again ranked China among the top three security threats and among the top three countries where they avoided doing business due to security threats.[93]

Several governments have expressed grave concerns about theft of trade secrets originating from China. In February 2013, the Executive Office of the President of the United States released a report on trade secret theft entitled "Administration Strategy on Mitigating the Theft of US Trade Secrets."[94] In addition to setting forth a strategy, the report gathered several previous US government assessments of the trade secret problem, including a 2011 report by

89 McAfee, Unsecured Economies: Protecting Vital Information 1, 2 (2009).

90 McAfee, Unsecured Economies: Protecting Vital Information 1, 12 (2009).

91 McAfee, Unsecured Economies: Protecting Vital Information 1, 13 (2009).

92 McAfee, Unsecured Economies: Protecting Vital Information 1, 14 (2009).

93 McAfee, Underground Economies: Intellectual Capital And Sensitive Corporate Data Now The Latest Cybercrime Currency 10 (2011).

94 Executive Office of the President of the United States, Administration Strategy on Mitigating the Theft of U.S. Trade Secrets (February 2013).

the Office of the National Counterintelligence Executive.[95] This report identifies China as posing a "pervasive threat" as one of the two most "aggressive collectors" (the other one identified was Russia) "of US economic information and technology."[96] In the days and weeks that followed release of the Administration Strategy, senior US officials frequently promoted the strategy and cited China (along with Russia) as a threat. Other governments have similarly singled out China as a source of trade secret theft.[97] For example, the head of Germany's military intelligence stated that one of his agency's main priorities was combatting industrial espionage from China and Russia.[98]

Reports and accusations of trade secret theft emanating from China have grown more specific in recent months as the US government has adopted a "naming and shaming" policy. For example, on 19 May 2013, the New York Times reported that Unit 61398, a 'cyberunit' of China's People's Liberation Army based in Shanghai had resumed attacks that "had stolen data from scores of American companies and government agencies."[99] According to the Times:

> The hackers were behind scores of thefts of intellectual property and government documents over the past five years, according to a report by [a security firm] in February that was confirmed by American officials. They have stolen product blueprints, manufacturing plans, clinical trial results, pricing documents, negotiation strategies and other proprietary information from more than 100 of [the security firm's] clients, predominantly in the United States. According to security experts, the cyberunit was responsible for a 2009 attack on the Coca-Cola Company that coincided with its failed attempt to acquire the China Huiyuan Juice Group.

One should note that concerns expressed by the US and other governments largely reflect a perception that Chinese entities are targeting trade secrets outside of China. Although these governments also complain that their citizens' trade secrets are threatened when doing business within China, addressing governments' issues with the strength and enforcement of trade secret laws *within* China would still not relieve their concerns about the actions of Chinese actors regarding trade secrets *outside* of China.

Commentary by Chinese experts is far more sanguine than the foreign perspective, but ultimately concedes and demonstrates the practical difficulty of proving a trade secret infringement claim and how it undermines the effectiveness of trade secret law in China. One expert commentary is typical. While acknowledging certain difficulties in enforcement, the commentators offered generally positive views:

---

95 Office of the National Counterintelligence Executive Report, Foreign Spies Stealing US Economic Secrets in Cyberspace (2011).

96 Ibid at 4 - 5.

97 Ibid at Appendix B-1.

98 Reuters, German Spy Chief Targets Russian, Chinese Industrial Espionage, 18 February 2013, http://www.reuters.com/article/2013/02/18/us-germany-spies-idUSBRE91H08C20130218.

99 D. Sanger and N. Perlroth, "Chinese Hackers Resume Attacks on US Targets," New York Times, A1, 19 May 2013, http://www.nytimes.com/2013/05/20/world/asia/chinese-hackers-resume-attacks-on-us-targets.html?_r=0.

> Over the past two decades, China has developed a comprehensive set of laws, regulations, and judicial interpretations designed to protect the rights of trade secret owners. Enforcement of trade secrets, however, is not straightforward. This is primarily because China does not have a US-style discovery system, and the evidentiary burden for a plaintiff to bring a trade secret misappropriation case in Chinese courts is relatively high. Notwithstanding the difficulties, there have been numerous cases of successful enforcement, both civil and criminal. Experience shows that it is possible to protect and enforce trade secrets in China, but the devil is in the details.[100]

Nevertheless, gathering evidence and proving a case appears to be difficult. These same commentators observed the difficulty of providing proof sufficient to obtain a preliminary injunction, which is typically considered essential in a trade secret case:

> Unlike a patent, trademark, or copyright, a trade secret is not a right granted by a government agency. Whether something constitutes a trade secret is almost always subject to disputes. As such, the likelihood of success on the merits is more difficult to prove for trade secret cases. Moreover, China has not adopted the inevitable disclosure doctrine. Therefore, it is rather unusual to obtain a preliminary injunction for trade secret misappropriation.[101]

Another commentator described the great difficulty in proving a trade secret case in China:

> The evidentiary requirements for court actions in China are very stringent. Little weight is generally accorded to affidavits and witness testimonies while physical evidence and documentary evidence are favoured. Such evidence is difficult to obtain in trade secret infringement cases. This problem is compounded by the problems relating to the lack of a discovery process in the PRC. In the PRC system, each party needs to adduce sufficient evidence to prove its claims. Although the court has the power to assist parties to gather evidence, such power is rarely used. Particularly when a rightholder is trying to gather evidence of infringement from an established infringer where it is often difficult to gain entry, there may be undue hardship for the rightholder.[102]

In sum, the overall picture of trade secret protection in China is mixed, with important challenges undermining the effectiveness of theoretically strong laws. Thus, laws are comprehensive, but appear to be somewhat difficult to navigate successfully. China is increasingly making intellectual property protection a priority,[103] but foreign businesses still perceive this protection poorly. This perception is disputed somewhat by local experts, but is nevertheless persistent. Even Chinese experts note that serious problems with evidentiary requirements and discovery make it difficult to obtain preliminary injunctions and to prove cases. Meanwhile, foreign governments perceive a serious threat to the trade secrets of their domestic industries coming from China.

---

100 Benjamin Bai & Guoping Da, Strategies for Trade Secrets Protection in China, 9 Northwestern Journal of Technology and Intellectual Property 351, 374- 375 (2011).

101 Ibid at 361.

102 Terrence F. MacLaren, Chiang Ling Li, 1 Trade Secrets Throughout the World § 8.52 (2012) (hereafter "MacLaren, Trade Secrets Throughout the World").

103 Benjamin Bai & Guoping Da, Strategies for Trade Secrets Protection in China, 9 Northwestern Journal of Technology and Intellectual Property 351, 374 - 375 (2011).

2. Scope and Subject Matter

There are several sources of trade secret law in China, with the primary one the Unfair Competition Law of 1993.[104] Other major sources include the Several Regulations Concerning Prohibition of Acts of Infringement of Trade Secrets ("Trade Secret Regulations") of 1998, pursuant to which the State Administration for Industry and Commerce enforces regulatory sanctions, and the Supreme People's Court Judicial Interpretation Regarding Various Issues in the Adjudication of Unfair Competitions Civil Cases (effective 2007) ("Unfair Competition Judicial Interpretation").[105] There are also numerous local regulations implementing the Unfair Competition law, including in Beijing Municipality, Guangdong Province, Hainan Province, Sichuan Province, Henan Province, Shenzhen Municipality, and Shanghai Municipality.[106] For the sake of maintaining a manageable, comprehensible scope, this summary will focus mainly on the Unfair Competition Law.[107]

a. Definitions

Chinese law defines trade secrets in terms similar to the laws of most countries. Article 10 of the Unfair Competition Law defines a "trade secret" as: "(1) Technical and business information that is unknown to the public (2) Which has economic value and practical utility; and (3) For which the trade secret owner has undertaken measures to maintain its confidentiality."[108] The Trade Secret Regulations, Article 2, contains this same definition.[109] Thus, under Chinese law, just like the law of many countries, a trade secret is commercially valuable technical or commercial information that is actually secret, and for which the owner takes reasonable measures to maintain secrecy. The information remains protectable as a trade secret for so long as it remains confidential. Once the information becomes public, trade secret protection ends.[110]

Like most countries, China requires the owner of the trade secret to make efforts to maintain secrecy. The Unfair Competition Judicial Interpretation of 2007 explains that such measures should be determined to be reasonable under the circumstances.[111] "It further states that courts shall determine whether the owner has adopted confidentiality measures according

---

104 Benjamin Bai & Guoping Da, Strategies for Trade Secrets Protection in China, 9 Northwestern Journal of Technology and Intellectual Property 351, 355 (2011); MacLaren, Trade Secrets Throughout the World § 8.3 (2012).

105 MacLaren, Trade Secrets Throughout the World § 8.3 (2012).

106 Ibid.; Shan Hailing, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, China 22 - 27 (2010).

107 For an easily accessible summary of several local regulations in English, see Shan Hailing, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, China 22 - 27 (2010), available as of 10 August 2013, at https://www.aippi.org/download/commitees/215/GR215china.pdf.

108 Article 10, Unfair Competition Law of the People's Republic of China (promulgated by the Standing Comm. Nat'l People's Cong., Sept. 2, 1993, effective Sept. 2, 1993, as translated in J. Benjamin Bai & Guoping Da, Strategies for Trade Secrets Protection in China, 9 Northwestern Journal of Technology and Intellectual Property 351, 355 - 356 (2011).

109 MacLaren, Trade Secrets Throughout the World § 8.4 (2012).

110 Ibid. § 8.5.

111 Benjamin Bai & Guoping Da, Strategies for Trade Secrets Protection in China, 9 Northwestern Journal of Technology and Intellectual Property 351, 359 (2011).

to the following factors: features of the relevant information carrier, confidentiality desire by the owner, identifiability of the confidentiality measures, difficulty for others to obtain it by justifiable means, and other factors."[112] The interpretation includes a non-exhaustive list of examples of potentially satisfactory security measures, which are relatively common, such as limiting access to secrets, posting confidentiality notices, and entering non-disclosure agreements.[113]

b. Scope and Subject Matter Under Civil Law

The scope of trade secret protection in China is broad. As noted in the definition above, it includes both confidential business information and technical information. Secrecy need not be absolute, and confidential information may be disclosed to others provided that the owner takes measures to protection secrecy.[114] Information must not be public or readily ascertainable from "common sense" or public sources, but absolute secrecy is not required.[115]

c. Scope and Subject Matter Under Criminal Law

The term "trade secrets" has the same meaning under the Criminal Code as it does under Article 10 of the Unfair Competition Law.[116] Thus, the definition, scope, and subject matter of trade secret appear to be the same between civil and criminal law.

3. Fault

a. Standard Under Civil Law

Article 10 of the Unfair Competition Act imposes liability on both common bases for trade secret liability: (1) misappropriation; and (2) breach of duty. Article 10 sets forth the following offenses:

- Acquiring trade secret of another by theft, inducement, duress, or other illegal means;
- Disclosing, using, or allowing others to use trade secret of another acquired by the above illegal means; or
- Disclosing, using, or allowing others to use trade secret in breach of an agreement or a confidentiality obligation imposed by a legal owner.[117]

Misappropriation thus consists of acquiring a trade secret by illegal or tortious acts, inducement of breach of duty, and other improper means, as well as disclosing, using, or allowing others to use a trade secret obtained by illegal or improper means. The catch-all

112 Ibid.

113 Ibid.

114 MacLaren, Trade Secrets Throughout the World § 8.5 (2012).

115 The Unfair Competition Judicial Interpretation of 2007 explains this issue in depth, providing guidance as to what is public and non-public. See Benjamin Bai & Guoping Da, Strategies for Trade Secrets Protection in China, 9 Northwestern Journal of Technology and Intellectual Property 351, 357 - 359 (2011); MacLaren, Trade Secrets Throughout the World § 8.5 (2012).

116 MacLaren, Trade Secrets Throughout the World § 8.9 (2012).

117 Article 10 of the Unfair Competition Law of the PRC. Translation from Benjamin Bai & Guoping Da, Strategies for Trade Secrets Protection in China, 9 Northwestern Journal of Technology and Intellectual Property 356 (2011).

category of "improper means" is not defined in the Act or subsequent interpretations. However, one authority opines that:

> It would seem that obtaining trade secrets by a party through any means other than conducting independent research and development, reverse engineering or obtaining the trade secrets in good faith from another party who is in possession of the trade secret in good faith would constitute obtaining trade secrets by other unfair methods.[118]

At the very least, improper means appear to include eavesdropping, espionage, or other means of circumventing measures expected to keep information confidential. For example, in a 1995 administrative action, a party was sanctioned for infringing trade secrets by intercepting phone calls to obtain customer information (identities and prices offered), which it used to steal customers.[119]

Breach of duty constitutes disclosing, using, or allowing others to use trade secret in breach of a duty to keep a trade secret confidential. Such a duty can arise in the context of an express agreement in the context of employment or a business relationship.[120] In business, a duty can arise in the context of contract negotiations, even if the contract is not concluded.[121] One expert noted that in the case of employees, it is not necessary to have an express confidentiality agreement – i.e., confidentiality obligations may be implied: "It is sufficient that the proprietor has communicated to the recipient of the trade secret its requirement to keep the information confidential."[122] As discussed elsewhere in this summary, however, commentators also stress how extremely difficult it is to prove trade secret claims. They encourage signed agreements, signed acknowledgements of receipt of trade secrets, and exit interviews where employees sign acknowledgements that they have received trade secrets.[123] For all practical purposes, therefore, it appears that an implied duty could rarely, if ever, be proven and thus does not exist. In addition, the Act provides for third party liability where a third party acquires, uses, or discloses trade secrets with knowledge or reason to know that they have been misappropriated or disclosed in breach of duty.[124]

---

118 MacLaren, Trade Secrets Throughout the World § 8.12 (2012).

119 MacLaren, Trade Secrets Throughout the World § 8.12 (2012).

120 MacLaren, Trade Secrets Throughout the World § 8.21 (2012) (discussing commercial agreements); MacLaren, Trade Secrets Throughout the World § 8.24 (2012) (discussing Article 22 of the Labour Law).

121 MacLaren, Trade Secrets Throughout the World § 8.21 (2012) (discussing Article 43 of China's Contract Law).

122 MacLaren, Trade Secrets Throughout the World § 8.14 (2012).

123 See MacLaren, Trade Secrets Throughout the World § 8.7 (2012); Benjamin Bai & Guoping Da, Strategies for Trade Secrets Protection in China, 9 Northwestern Journal of Technology and Intellectual Property 356, 362 - 363 (2011).

124 Article 10 of the Unfair Competition Law of the PRC. See Benjamin Bai & Guoping Da, Strategies for Trade Secrets Protection in China, 9 Northwestern Journal of Technology and Intellectual Property 356 (2011).

Independent creation and reverse engineering are both defences to trade secret infringement.[125] A party that has obtained a secret by improper means may not invoke the defence of reverse engineering.[126]

b. Standard Under Criminal Law

Chinese criminal law imposes liability for intentional trade secret theft pursuant to Article 219 of the criminal law. Both the definition of trade secret and the scope of acts covered by the criminal law is the same as under Article 10 of the Unfair Competition Law.[127] Given the nature of these acts, the defendant appears to need intent, except when receiving trade secrets that are wrongly procured or disclosed, where a reason to know of their status will suffice. "However, an act of infringement of trade secrets will only amount to a crime under Article 219 of the Criminal law if the infringing act causes . . . "serious losses" or "extremely serious consequences" to the proprietor."[128] The amount of losses necessary appears to now be defined, since 2011 when:

> the Supreme People's Procuratorate and the Ministry of Public Security jointly issued new regulations relating to filing criminal cases. Under the new regulations, in cases of trade secret infringement, a criminal investigation and prosecution shall proceed under any of the following circumstances:
>
> 1. Losses of more than RMB 500 000 are caused to the owner of the trade secret;
>
> 2. The amount of illegal gains from infringement is more than RMB 500 000;
>
> 3. The owner of the trade secret becomes bankrupt due to the infringement; or
>
> 4. The infringement causes other grave losses to the owner of the trade secret.[129]

Criminal prosecutions may be difficult to obtain. One authority notes:

> Generally speaking, criminal prosecution is very effective in trade secret misappropriation cases, but it is not always easy to get police interested in run-of-the-mill trade secret cases. In the authors' experiences, the police are more interested in high profile cases. Consequently, the authors advise that one should try to "package" the case as "high profile" to enhance the chance of criminal prosecution. It also is important to build good relationships with the local community, including the local police, before any misappropriation happens.[130]

125 Article 12 of the Unfair Competition Law of the PRC. See Benjamin Bai & Guoping Da, Strategies for Trade Secrets Protection in China, 9 Northwestern Journal of Technology and Intellectual Property 351, 360 (2011).

126 Article 12 of the Unfair Competition Law of the PRC. See Benjamin Bai & Guoping Da, Strategies for Trade Secrets Protection in China, 9 Northwestern Journal of Technology and Intellectual Property 351, 360 (2011).

127 MacLaren, Trade Secrets Throughout the World § 8.9 (2012).

128 Ibid.

129 Ibid.

130 Benjamin Bai & Guoping Da, Strategies for Trade Secrets Protection in China, 9 Northwestern Journal of Technology and Intellectual Property 351, 365 (2011).

4. Remedies

a. Remedies Under Civil Law

Chinese law provides remedies including compensatory damages in the form of a plaintiff's lost profits, a defendant's profits gained, and a reasonable royalty.[131] Consequential damages are available as well, where the defendant has caused the trade secret to become public.[132]

As previously noted, injunctions are available, but it is unusual to obtain one in a trade secret case, and they are thus, in effect, unavailable.[133] One expert observes the following:

> However, in cases involving trade secrets and other intellectual properties, the applicability of the preliminary [injunction] is weak and its application is very limited in such cases. This is mainly because the conditions for preliminary execution are hard to meet in law suits involving trade secrets. Article 98(1) of the Civil Procedure Law provides that cases in which preliminary execution is ordered by the people's court shall meet the condition that the relationship of rights and obligations between the parties is definite, and that denial of preliminary execution would seriously affect the life or business of the applicant. This requires the applicant and the judge to explain, in order to support the adoption of a preliminary execution order, why, in the absence of such order, the production or business operation of the applicant will be seriously affected. However, cases involving trade secrets are often complicated. The parties have substantial disagreements on whether the trade secret of the plaintiff exists, whether the defendant's activity has been based on such trade secret or just on common knowledge, experience and skills of the defendant, etc. The rights and obligations between the plaintiff and the defendant are not clear. Furthermore, a lot of trade secrets cost little to form, contain little originality, are often not in use or belong to negative information, which, even if used by others, will not seriously affect the life or business of the right holder. Therefore, it is difficult for the plaintiff to apply for preliminary execution in these cases.[134]

This difficulty in obtaining a preliminary injunction appears to arise from the standards set forth in the Civil Procedure Law generally. The same expert quoted above observes that China has amended its copyright, patent, and trademark laws so that Chinese law is "in conformity with the requirement on provisional measures contained in" Article 50 of TRIPS.[135] However, the expert further observes that "trade secrets have not received similar treatment. No new

131 Ibid at 361.

132 Ibid.

133 Ibid; Shan Hailing, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, China 34 - 35 (2010), available at: https://www.aippi.org/download/commitees/215/GR215china.pdf.

134 Shan Hailing, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, China 35 (2010), available at: https://www.aippi.org/download/commitees/215/GR215china.pdf.

135 Ibid.

civil remedy measure has been added. The old regulation of the 1991 Civil Procedure Law was left unchanged."[136]

By contrast, permanent injunctions are routinely granted – where a plaintiff proves its case.[137] However, they are not granted automatically.[138] Moreover, court may choose instead to limit the scope and length of an injunction to a "reasonable" amount of time "provided that the trade secret owner's competitive advantages are legally protected."[139] A court may also order return of the trade secrets and media containing them.[140]

b. Remedies Under Criminal Law

Chinese law provides for both administrative and criminal sanctions. Under the Unfair Competition Act, authorities from the offices of the Administration for Industry and Commerce may investigate and sanction trade secret misappropriation. They may issue fines of between RMB 10 000 and RMB 200 000. [141] They may also order the return of materials containing the trade secrets and order the destruction of the infringing goods made using the stolen trade secrets.[142] Criminal sanctions apply to those who cause "serious" or "exceptionally serious" losses through trade secret theft. "Serious" losses of RMB 500 000 or more incur a jail sentence of up to three years. "Exceptionally serious" losses of RMB 2 500 000 or more warrant a sentence of three to seven years.[143] Fines also apply, but amounts are not specified.

5. Procedures

a. Emergency Action to Preserve Proof

Under Article 74 of the Chinese Civil Procedure Code, a party may apply to the court for an order for the preservation of evidence.[144] Ex parte orders are available. These actions are usually undertaken by the judge, and may include orders to produce documents immediately, inspections, and orders to produce documents.[145] Evidence preservation orders has become a "routine "and "powerful tool in trade secret misappropriation cases in Chinese courts."[146] "According to the statistics released by the Supreme People's Court, Chinese courts granted

136 Ibid.

137 Benjamin Bai & Guoping Da, Strategies for Trade Secrets Protection in China, 9 Northwestern Journal of Technology and Intellectual Property 351, 361 (2011).

138 Ibid.

139 Ibid.

140 MacLaren, Trade Secrets Throughout the World § 8.26 (2012).

141 Benjamin Bai & Guoping Da, Strategies for Trade Secrets Protection in China, 9 Northwestern Journal of Technology and Intellectual Property 351, 361 - 362 (2011).

142 Benjamin Bai & Guoping Da, Strategies for Trade Secrets Protection in China, 9 Northwestern Journal of Technology and Intellectual Property 351, 361 - 362 (2011).

143 Ibid at 364 – 365.

144 Ibid at 363 – 364.

145 Ibid.

146 Ibid.

93.72% of the 1,312 motions for evidence preservation in IP-related cases from 2002 to 2009."[147]

b. Pre-Trial Disclosure and Discovery

There is no ordinary pre-trial discovery available to plaintiffs in civil cases. However, plaintiffs often take advantage of the procedure for the preservation of evidence available under Article 74 of the Chinese Civil Procedure Code as well as findings from administrative or criminal investigations.[148] Nevertheless, this lack of discovery poses a great difficulty for plaintiffs, particularly given the preference of Chinese courts for original, documentary evidence over testimony and affidavits.[149] One expert opinion observes the effects:

> Because there is no US-style discovery in China, plaintiffs must collect and submit their own evidence to meet their burden of proof regarding, inter alia, trade secret misappropriation and damages. Chinese courts rarely accept evidence unless in its original form; therefore, documentary evidence is practically the only form of evidence that carries significant weight in a Chinese court. However, evidence obtained in violation of law is inadmissible in Chinese courts, and if admitted, it may constitute reversible error on appeal. Subsequently, it is essential to have a proper and thorough evidence gathering strategy to overcome the challenging evidentiary hurdles for a potential plaintiff in a trade secret misappropriation case. In some cases, it is challenging to obtain documentary evidence to prove misappropriation. In others, it may be difficult to prove that the potential defendant had access to confidential information.[150]

These evidentiary challenges lead experts to consistently recommend confidentiality agreements as absolutely necessary to protect trade secrets.[151] As noted above, such agreements are also advised due to the (likely insurmountable) difficulty of obtaining a preliminary injunction, where "the relationship of rights and obligations between the parties [must be shown to be] definite."[152] However, even a written agreement is likely not enough:

> As a practical result, though trade secrets can be protected by means similar to those used in the US, such as a confidentiality agreement, the mere existence of a confidentiality agreement may not be sufficient. It is advisable to have the recipient sign an acknowledgement of receiving access to the confidential information, in addition to executing a confidentiality agreement, prior to giving confidential information to a recipient.[153]

---

147 Ibid.

148 Ibid; MacLaren, Trade Secrets Throughout the World § 8.52 (2012).

149 MacLaren, Trade Secrets Throughout the World § 8.52 (2012).

150 Benjamin Bai & Guoping Da, Strategies for Trade Secrets Protection in China, 9 Northwestern Journal of Technology and Intellectual Property 351, 362 - 363 (2011).

151 See ibid; MacLaren, Trade Secrets Throughout the World § 8.7 (2012); Shan Hailing, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, China 10, 27, 34 (2010), available at https://www.aippi.org/download/commitees/215/GR215china.pdf.

152 Shan Hailing, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, China 35 (2010), available at https://www.aippi.org/download/commitees/215/GR215china.pdf.

153 Benjamin Bai & Guoping Da, Strategies for Trade Secrets Protection in China, 9 Northwestern Journal of Technology and Intellectual Property 351, 363 (2011).

Thus, not only is pre-trial discovery non-existent for trade secret cases, but evidentiary burdens are extremely high, making it difficult to prove a case.

It appears reasonable to conclude that a de facto set of formalities exist with respect to trade secrets in China, because of the lack of discovery, the preference for specific, original documentary evidence establishing the existence of a trade secret, and the consistent recommendations of experts. At least this is the case with respect to trade secret suits where breach of duty, or inducement of breach of duty, is alleged, rather than outright theft. To successfully avail themselves of the laws on the books in a case involving breach of duty, plaintiffs must describe the trade secret in writing, obtain written agreements protecting its confidentiality, and obtain written acknowledgement of its receipt.

c. Secrecy During Litigation

The Chinese Civil Procedure Law provides measures for preserving the confidentiality of trade secrets during litigation. Files can be kept confidential and in-camera hearings are available upon the request of a single party.[154] However, there is not protection from the other party.[155] Moreover, the in-camera hearing protection is not comprehensive, as it excludes only the general public and "mass media, which still opens [the hearing] to all litigant participants, including judicial officers, court clerks, plaintiffs, defendants and their agents."[156]

6. Employee-Employer Relationships

Employers may enter agreements with employees to keep information confidential in accordance with the Labour Contract Law of 2008.[157] "Whenever possible, confidentiality agreements should clearly identify the information that the employer deems as confidential."[158] No fixed term of confidentiality is required, but it is expected that such obligations terminate when the information becomes public.[159]

Non-competition agreements are permissible, subject to certain limitations:[160] They are enforceable only with respect to senior management, senior technical personnel, and employees who had a confidentiality obligation. They must specify monthly compensation for the term of the non-compete. The period may not exceed two years after employment.

154 Shan Hailing, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, China 35 - 36 (2010), available at: https://www.aippi.org/download/commitees/215/GR215china.pdf.

155 MacLaren, Trade Secrets Throughout the World § 8.47 (2012).

156 Shan Hailing, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, China 36 (2010), available at: https://www.aippi.org/download/commitees/215/GR215china.pdf.

157 MacLaren, Trade Secrets Throughout the World § 8.24 (2012).

158 Benjamin Bai & Guoping Da, Strategies for Trade Secrets Protection in China, 9 Northwestern Journal of Technology and Intellectual Property 351, 368 (2011).

159 See ibid.

160 MacLaren, Trade Secrets Throughout the World § 8.24 (2012).

Between companies, non-competes are viewed with scepticism. Not only are they subject to competition authority scrutiny, but even in the case of an acquisition, the pro-competitive benefits must outweigh the harms.[161]

7. Data Protection and Exclusivity

China protects undisclosed test data of pharmaceutical and agricultural products containing a new chemical entity for six years from the date of marketing approval. During this time, no other party can use the data submitted as the basis for an application.

This protection is limited in practice with respect to pharmaceuticals. Data exclusivity in such cases is limited to the data provided, and does not provide marketing exclusivity (i.e. exclusive rights to market the drug). China is apparently willing to rely on approval granted in other countries to approve drugs, thus rendering the issue of data exclusivity somewhat moot. Specifically, the Pharmaceutical Research and Manufacturers of America trade association (PhRMA) has complained that:

> [I]n practice, China grants [regulatory data protection] only to pharmaceutical products that are "new" to the world – in other words introduced first in China. . . . China's regulatory procedures permit the SFDA to grant marketing approval to products that have previously been approved outside of China. Non-originator applicants can effectively rely on the originator's overseas marketing approval to meet their requirements for obtaining marketing approval in China . . . China's open reliance on the originator's overseas marketing approval allows a subsequent manufacturer the ability to gain marketing approval in China.[162]

8. Complementary Legal Institutions

On the Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, China receives a score of 6.2 out of 10, which ranks it 49th in the world.[163] Its lowest scores are with respect to judicial independence (4.9 out of 10) and impartial courts (5.2 out of 10).[164]

9. Technology Transfer

China continues to maintain significant regulations on the transfer of technology under both national and local regulations. These include rules giving employees a "veto" over the transfer of technology they develop as well as registration and regulation of in-bound technology transfer agreements. However, the regulations are less demanding than in the past and less targeted at termination and transfer of trade secrets than they once were.

---

161 Ding Liang, The Interplay of Non-compete Covenants under the PRC Anti-monopoly Law, King Wood & Mallesons China Bulletin (April 2008), http://www.kingandwood.com/article.aspx?id=The-Interplay-of-Non-compete-Covenants-under-the-PRC-Anti-monopoly-Law-04-china-bulletin-2008&language=en.

162 Pharmaceutical Research and Manufacturers of America (PhRMA) Special 301 Submission 2013, available at: http://www.phrma.org/sites/default/files/pdf/PhRMA%20Special%20301%20Submission%202013.pdf.

163 Fraser Institute, Economic Freedom of the World 2012 Annual Report at 56 (2012).

164 Ibid.

In China, an employee has certain inalienable rights with respect to technology created by that employee during the course of his employment. Although such technology belongs to the employer, the employee must be compensated (beyond his salary) for the use or transfer of such technology.[165] Moreover, the employee has the right of first refusal regarding any license of assignment of the technology.[166]

Technology import contracts of technology must be recorded, but generally need not be pre-approved.[167] Any change requires a new recordation.[168] Certain technology is prohibited from importation, while other restricted technology must be licensed.[169] "Where foreign investors contribute technology as capital contribution to foreign-invested enterprises, the licensing or assignment of such technology is to be approved in accordance with the examination and approval procedures for the establishment of foreign-invested enterprises."[170]

The law imposes a large number of substantive requirements on technology import contracts. Among these requirements are that they must contain the following provisions:[171]

- Various warranties regarding the ownership and efficacy of the technology.
- Confidentiality obligations terminate when information is disclosed publicly by an unrelated third party.
- May not tie the license to unrelated conditions such as the purchase of goods or services.
- May not contain obligations with respect to technology covered by an expired patent.
- May not restrict the transferee from improving technology of from using such improvements (even though the licensor may stipulate ownership of improvements).
- May not prohibit transferee from obtaining the technology from alternate sources.
- No unreasonable restrictions on quantity, sales price, or other aspects of transferee's products.
- No unreasonable restrictions on export of products made by the transferee using the technology.
- Improvements developed pursuant to a joint development or commission agreement belong to the developer, unless expressly agreed otherwise.[172]

Certain earlier, more burdensome restrictions have been eliminated.[173] These included limits on the term of the license, the right of the licensee to continue use of the technology after the term of the license, and restrictions on the period of confidentiality.

165 MacLaren, Trade Secrets Throughout the World § 8.24 (2012).

166 Ibid.

167 Ibid at § 8.36.

168 Ibid at § 8.37.

169 Ibid at § 8.35.

170 MacLaren, Trade Secrets Throughout the World § 8:37 (2012).

171 Ibid at § 8.34.

172 Ibid at § 8.32.

173 Ibid at § 8.34.

France

1. Overview

French law protects trade secrets through both civil and criminal law, but in limited, isolated ways. There is no comprehensive legislation covering all trade secrets. Rather, French law addresses only one category of trade secrets—manufacturing secrets—through specific criminal law legislation, and in that instance, the secrets are protected only in certain circumstances. Authorities and trade secret owners use other categories of generally applicable civil and criminal law to protect trade secrets, but the coverage of the law is not comprehensive. As a recent parliamentary report noted, "legislation relative to unfair competition applies only in conditions which are difficult to bring together and which are not particularly restrictive for violators."[174]

French trade secret protection is not viewed as effective by some experts. Stouls et al. (2010) sum up this view:

> [T]here have been relatively few examples of case law over the past decade and, in case of conviction, but for exceptions, the penalties which are imposed are limited to modest damages; prohibition of use is quite rare. . . . This might lead one to think that the protection of trade secrets in France would not generally be very effective.[175]

They further remark that greater protection during litigation would be desirable:

> The difficulties of ensuring the preservation of the secrets of one or more parties to a proceeding and, in particular, the difficulty of getting the judge to order a measure of confidentiality prohibiting the parties from disclosing to third parties the documents transmitted, the obligation, in order to obtain closed proceedings, for this to be requested by all the parties, and the impossibility for the judge to limit access to judgements or to draft several versions of his judgement (a confidential version for the parties and an expurgated version which would be the only one accessible to third parties).[176]

2. Scope and Subject Matter

French law recognizes three categories of trade secrets: (1) manufacturing secrets (or *secrets de fabrique*); (2) confidential business information; and (3) know-how (or *savoire-faire*). Only manufacturing secrets are expressly protected, pursuant to criminal law related to Labor contracts.

a. Definitions

- Manufacturing Secrets

French law imposes criminal liability on managers and employees of a business for unauthorized disclosure of that business' manufacturing secrets pursuant to Article L. 1227-1

174 Jean-Pierre Stouls et al., Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, France 1 (2010).

175 Ibid.

176 Ibid at 25.

of the Labor Code[177] and Article L. 621-1 of the Intellectual Property Code[178] (which essentially incorporates the relevant provision from the Labor Code). However, neither section defines "manufacturing secrets."

The French courts have defined manufacturing secrets as commercially valuable processes, devices, or inventions related to manufacturing that are kept secret by the manufacturer. For example, the High Court, or *Cour de Cassation*, has described a manufacturing secret generally as a "manufacturing process which has a practical or commercial interest and which the manufacturer keeps hidden from its competitors" [179] In other cases, courts have recognized the definition as including the following subject matter related to manufacturing: methods or inventions,[180] improvements of older processes, [181] or the use of a particular device[182] or software[183] in the manufacturing process.

A manufacturing secret is protected as such only for so long as it remains secret. Once it is known to third parties or falls into the public domain, it is no longer protected. If a secret is ascertainable from reverse engineering, then it is not protected under law.[184] The manufacturer must take precautions to protect secrecy, including notifying employees of the need to keep secrets and protecting against inadvertent disclosure. However, a secret need not be kept absolute. It may be shared with employees as needed, as well as pursuant to a license agreement.

- Confidential Business Information

There is no legislation defining confidential business information, nor does case law offer a comprehensive definition. A leading treatise[185] compiled the following list of examples from cases and commentaries:

- Information concerning the commercial organization of a company, such as network of distributors;
- The text of confidential commercial contracts and commercial arrangements;

177 "Every manager or employee of a business who communicates or attempts to communicate a trade secret, may be punished by imprisonment of two years and by a fine of EUR 30 000. The court may also decide as additional punishment, for five years at most, to suspend civic, civil and family rights, as provided for in Article 131-26 of the Criminal Code." Labour Code Article L. 1227-1 Translation from MacLaren, Trade Secrets Throughout the World § 14:3 (2012).

178 "The penalties for violation of manufacturing secrets are set forth in Article L.1227-1 of the Labor Code reproduced hereafter: [quotes Labor Code Article L. 1227-1 in whole].

179 Cass. crim., 19 September 2006, No. 05-85360, translation from MacLaren, Trade Secrets Throughout the World § 14:4 (2012).

180 Cass. crim., 29 March 1935, Gaz. Pal. 1935, 1, 928.

181 Court of Appeals of Paris, 20 February 1863, Ann. Propr. Ind. Litt. & Art. 1876.179. CAA Nancy, 3 July 2003, No.98NC01900.

182 Tribunal correctionnel de la Seine, February 22, 1926, Ann. Propr. Ind. Litt. & Art. 1926. Cass. crim. June 12, 1974, No. 73-90.724.

183 Revue Lamy "Droit de L'immatériel," 2007 No. 27, 05-2007. To be clear: The software must be an accessory to a manufacturing process.

184 Cass. com. 22 March 1971, Bull. Civ. IV, No. 84.

185 The list is quoted in its entirety from 2 Trade Secrets Throughout the World § 14:6

- Internal policy regulations and communications;
- Information concerning sales, sales policy, discounts, commissions, sales forecasts, profitability forecasts, etc.;
- List of names and addresses of clients, agents and particulars of each;
- Financial plans;
- Information as to investments;
- Cost figures and calculations;
- Banking relationships;
- Legal disputes with employees, clients, etc.;
- Lists of suppliers;
- Set-up of distribution networks;
- Credit of a business;
- Methods of research and marketing;
- Accounting methods; and
- Comparative charts of audience rating for radio and television channels.

Confidential business information must be kept confidential. Thus, it must not have fallen into the public domain. Moreover, the business must ensure that proper precautions against disclosure are taken.

- Know-How or Savoir Faire

Know-how is "knowledge acquired through experience, for which a person who wishes to save money and time is ready to pay a certain amount of money."[186] More generally, the importance of this category appears to be that it describes a category of commercially valuable secrets much broader than manufacturing processes or technical information. It includes knowledge of methods, processes, and information regarding management, finance, and commercial relations.[187] Know-how must be kept confidential to qualify for protection. Thus, it must not have fallen into the public domain. Moreover, the business must ensure that proper precautions against disclosure are taken.

b. Scope and Subject Matter Under Civil Law

Civil law provisions used against trade secret infringement include breach of contract actions pursuant to Article 1147 of the Civil Code. Contract law is used only where a person has a contractual obligation to keep information secret.

Absent a contractual obligation, tort law[188] can be used to protect trade secrets. Under French law, a party can bring an action for unfair competition against a competitor that

186 MacLaren, Trade Secrets Throughout the World § 14:7 (2012).

187 Ibid.

188 Art. 1392 of the Civil Code: "Any act whatsoever of one person, which causes damage to another, obliges the one by whose fault it occurred, to put it right." Hogan Lovells International LLP, Report on Trade Secrets for the European Commission Appendix 2 at 66 (2012).

misappropriates trade secrets. Such unfair competition includes bribing or paying a competitor's employees to reveal secrets or hiring a competitor's employee to obtain a secret. The use of a wrongfully-obtained trade secret is also unfair competition. However, independent development of one's own confidential information or know-how is permissible.

c. Scope and Subject Matter Under Criminal Law

- Manufacturing Secrets

As described above, French law protects Manufacturing Secrets as defined in the previous section. It is important to note an essential limitation of the statutory provisions protecting Manufacturing Secrets. The provision applies to *disclosure* (or attempted disclosure) by an *employee* or *manager*. It thus applies to disclosure only, not to use by the employee for his own benefit. The provision also does not apply to any third parties (other than former employees who obtained the secret during employment).

- Confidential Business Information and Know-How

Several generally-applicable provisions of French criminal law have been used to protect confidential business information, know-how and manufacturing secrets (where they are not already protected by specific criminal legislation as described above).[189] These include prohibitions against fraud, theft[190] (of the physical embodiment of trade secrets), and breach of professional obligations of confidentiality[191] (e.g. a doctor's duty to keep confidences). These provisions have been applied both to individuals who wrongly disclosed information and to those in receipt. Thus, a trade secret can be protected indirectly at criminal law through protection of its physical embodiment – a party who takes documents or computer media containing trade secrets can be prosecuted. Moreover, where a professional obligation exists (e.g. in the case of doctors and lawyers), breach of confidence may result in criminal prosecution.

One important and significant recent development in French criminal law is the use of prohibitions against breach of trust to prosecute trade secret misappropriation (whether it was manufacturing secrets, confidential business information, or know-how).[192] Art 314-1 of the Criminal Code states that "Breach of trust is the act of a person's misappropriating, to the prejudice of others, funds, securities or any property transmitted to him and which he accepted while being responsible for returning them, representing them, or using them in a specific way. Breach of trust is punished by three years of imprisonment and a fine of 375 000 Euros".[193]

189 Hogan Lovells International LLP, Report on Trade Secrets for the European Commission, Appendix 2 at 66 (2012).

190 Art. 311-1 of the Criminal Code: "Theft is the fraudulent appropriation of a thing belonging to another person." Translation from Hogan Lovells International LLP, Report on Trade Secrets for the European Commission, Appendix 2 at 67 (2012).

191 Art. 226-13 of the Criminal Code: "The disclosure of information of a secret nature under a person's custody either by reason of his office or his profession, or because of a position or temporary assignment, is punished by one year of imprisonment and a fine of 15 000 Euros." Translation from Hogan Lovells International LLP, Report on Trade Secrets for the European Commission, Appendix 2 at 67 (2012).

192 Christophe Garin, "Customer poaching can now be punished by criminal courts on the ground of breach of trust," Lexology (24 May 2012) at: http://www.lexology.com/library/detail.aspx?g=e11830fd-5222-4084-afdd-a160047f2fec.

193 Art 314-1 of the Criminal Code. Translation from Hogan Lovells International LLP, Report on Trade Secrets for the European Commission, Appendix 2 at 67 (2012).

For example, Article 314-1 of the Criminal Code, which addresses breach of trust was used to prosecute a Michelin employee in 2010 who attempted to sell technology to a competitor.[194] In late 2011, the French Supreme Court extended Section 314-1 to include information in the goods or property protected by Section 314-1. In *Poruvois*, Cass. crim., 16 November 2011, no. 10-87.866, the Court held that the appropriation of customer lists by a former employee could constitute breach of trust. The Court reasoned that "the provisions of this text apply to any goods, which may be appropriated" and that "the information relating to customers constitutes a good that may be misappropriated."[195] This case marks the culmination of an evolution of case law starting in 2000 where the court increasingly applied Section 314-1 to intangible goods, starting with bank card numbers, internet access, and then an industrial "project" without reference to a physical medium.[196]

Breach of trust pursuant to Art. 314-1 thus now appears to offer a viable tool for prosecuting trade secret misappropriation. It does, however, have a significant limitation. The alleged mis-appropriator must have been in a position of trust, with some prior obligation relating to the property. People fitting into this category appear most likely to be parties who have agreed to such an obligation, or parties for whom such an obligation is implicit, such as employees, agents, or professionals.

In sum, French criminal law is most likely to punish the misappropriation of trade secrets by employees or other parties with a prior relationship with the trade secret owner. A third party who misappropriates trade secrets will be criminally liable only by virtue of a related wrongful act, such as theft of tangible property (papers, models or computer disks) or fraud.

3. Fault

a. Civil Law

A party using tort law to combat trade secret misappropriation need only show fault, damage and causation.[197] Thus, proof of intent is not necessary and negligence may suffice.

b. Criminal Law

Article L. 1227-1 of the Labor Code[198] and Article L. 621-1, which apply to employee disclosure of manufacturing secrets, requires intentional disclosure to a third party of information that the discloser knows or should know is confidential. Generally, uses of laws

194 Hogan Lovells International LLP, Report on Trade Secrets for the European Commission, Appendix 2 at 67 (2012), citing Tribunal Correctionnel de Clermont-Ferrand, 21 June 2010).

195 Translation from Christophe Garin, "Customer poaching can now be punished by criminal courts on the ground of breach of trust," Lexology (24 May 2012) at: http://www.lexology.com/library/detail.aspx?g=e11830fd-5222-4084-afdd-a160047f2fec.

196 Ibid.

197 Hogan Lovells International LLP (2012), Report on Trade Secrets for the European Commission, Appendix 2.

198 "Every manager or employee of a business who communicates or attempts to communicate a trade secret, may be punished by imprisonment of two years and by a fine of € 30,000. The court may also decide as additional punishment, for five years at most, to suspend civic, civil and family rights, as provided for in Article 131-26 of the Criminal Code." Labour Code Article L. 1227-1 Translation from MacLaren, Trade Secrets Throughout the World § 14:3 (2012).

against breach of trust, theft, misappropriation, fraud or other criminal acts to prosecute trade secret theft also require a showing of intent.[199]

4. Remedies

a. Civil Law

Remedies under French law include compensatory damages, lost profits, moral damages (e.g. loss of reputation), legal expenses, injunctive relief, destruction of infringing goods and preliminary injunctive relief.

b. Criminal Law

Under the Articles that apply to manufacturing secrets, Article L. 1227-1 of the Labor Code and Article L. 621-1 of the IPC, a convicted infringer faces 2 years imprisonment and a fine of 30 000 Euros. Other penalties for generally applicable laws used to prosecute trade secret theft come with potential imprisonment and substantial fines. For example, a breach of trust can be punished, pursuant to Article 314-1 of the Criminal Code with a 3 year prison sentence and a 375 000 Euro fine. A third party who receives stolen information can be punished under Article 321-1 of the Criminal Code with 5 years of imprisonment and a 375 000 Euro fine.

5. Procedures

a. Emergency Action to Preserve Proof

Article 145 of the French Code of Civil Procedure (FCCP) provides for summary (i.e., ex parte) proceedings to preserve proof of suspected wrongdoing.

b. Pre-Trial Discovery

Pre-trial discovery is limited to documentary evidence and is conducted under the direction of the judge. Under Articles 11 and 138 - 141 of the FCCP, a Court may order the production of documents and other evidence necessary for a party to prove its case, including from third parties.

c. Secrecy During Litigation

French civil procedure contains several procedures that run counter to the need to protect trade secrets during litigation.[200] It requires access by the parties to documents; open courts; and the public pronouncement of judgments.

On the one hand, documents in the case are available only to the parties. On the other hand, access to documents by the parties is largely unrestricted unless the parties agree to restrain themselves or the court makes an exceptional ruling.[201] In-camera hearings cannot occur unless all parties request them.[202] The judgment must be publically available. “There are no legal or statutory provisions enabling the court to restrict access to its judgment, nor to draft two versions of its decision, a complete decision for the parties and an expurgated version

199 Hogan Lovells International LLP (2012), Report on Trade Secrets for the European Commission, Appendix 2, at 69 (2012).

200 J.-P. Stouls et al., Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, France 16 (2010).

201 Ibid at 17.

202 Ibid at 18.

accessible to third parties"[203]. As one commentator observed, "[i]t will appear that French civil proceeding rules may not be sufficient to ensure that the secrets of one or more parties to a civil action are preserved."[204]

6. Employee-Employer Relationships

During employment, employees may not disclose their employer's trade secrets. After employment, they remain under a duty not to disclose the former employer's secrets. "Nonetheless, case law (Paris 23 March 1982, in particular) admits that in his new duties, a former employee is free to use the know-how and experience gained in his previous employment."[205] Thus, a distinction is made between general skills and experience (unprotectable) and the specific secrets of the former employer (protectable).

Covenants not to compete are generally enforceable during and after the term of employment, but must be weighed against the employee's right to make a living.[206] The clause must appear in the employment contract, it must be limited in time and place, and it must provide financial remuneration, it must take the facts of the employee's situation into account.[207]

7. Data Exclusivity and Data Protection

France has implemented the standard EU approach to protection of test data for pharmaceuticals set forth in EU Directive 2001/83/EC as amended by EU Directive 2004/27/EC. This approach is known as the "8 + 2 + 1 year approach." Pharmaceutical test data submitted to government for new medicinal products and new indications or uses is protected from disclosure or use for 8 years. Once the 8 year period ends, the data can be used by generic manufacturers to prepare and apply for regulatory approval, but not market a product. This period of market exclusivity lasts 2 years. The initial applicant may receive another 1 year for new indications.

8. Complementary Legal Institutions

France's commercial legal system is generally well-regarded. On the Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, France receives a score of 7.96 out of 10, which ranks it 24th in the world.[208] It ranks relatively highly with respect to most subcomponents of the index.

9. Technology Transfer

France does not subject foreign investors to technology transfer requirements, joint venture technology contribution requirements, or license registration requirements.[209]

---

203 Ibid.

204 Ibid at 17.

205 Ibid at 24.

206 MacLaren, Trade Secrets Throughout the World § 14:27 (2012).

207 J-P. Stouls et al., Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, France 24 (2010).

208 Fraser Institute, Economic Freedom of the World 2012 Annual Report at 74 (2010).

209 MacLaren, Trade Secrets Throughout the World § 14:35 (2012).

Germany

1. Overview

Germany has no single civil or criminal statute that covers trade secrets comprehensively, but does essentially provide comprehensive protection through a large number of provisions in both criminal and civil law that specifically address trade secrets. The most significant of these are the criminal provisions in the Act Against Unfair Competition of 1909 (UWG). Commentators have characterized the German system of trade secrets as particularly complex in comparison to other countries because of the number and interaction of different statutes.[210]

The most significant limitation on trade secret law enforcement in Germany appears to be procedures in civil cases, which make it difficult to prove a case and to protect confidential information while doing so. In civil cases, the trade secret must be pled with specificity, which may be difficult, and, more important, may expose the trade secret to public disclosure. As an expert report observes:

> [I]t is also problematic that in cases where claims are asserted on the basis of a trade secret the secret information must be identified and its content must be described. This involves the risk that the trade secret finally becomes common property or becomes known to the opposing party in more detail. Hence, protection of know-how in (infringement) proceedings has to be assessed as insufficient.[211]

The requirement of specificity can also prevent effective relief. For example, a motion for a preliminary injunction where documents containing trade secrets were copied would need to specify the relevant documents to be secured and handed over. As another expert report observes, this requirement presents a challenge:

> One specific difficulty is to precisely identify the relevant trade secrets in the motions of any given action (cease and desist motions, motions to handover documentation etc.). According to German law of civil procedure, every motion must be specific enough that there is no doubt as to whether a certain document is covered or not.[212]

Exacerbating the effect of this requirement is that trade secrets are not well protected in the course of litigation as discussed below. Also, pre-trial discovery is not available, making proof difficult. Because of these limitations, German plaintiffs often seek the initiation of a criminal case first before following with a civil case. As discussed below, however, criminal protection is also limited in significant ways.

2. Scope and Subject Matter

a. Definitions

German law and legal practice recognizes three categories of trade secrets: industrial secrets (Betriebsgeheimnis), commercial secrets (Geschaeftsgeheimnis), and know-how. The terms Betriebsgeheimnis and Geschaeftsgeheimnis are used by statutes, while the term

210 MacLaren, Trade Secrets Throughout the World § 15:1 (2012), citing, in turn, 3 Trade Secrets and Know-how throughout the World, paragraph 4.04 [2].

211 M-R. McGuire et al., Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, Germany 22 - 27 (2010).

212 Hogan Lovells International LLP, Report on Trade Secrets for the European Commission, Appendix 2, at 91 – 92.

know-how, which is not a statutory term, is used frequently in legal practice in licenses and contracts. German law makes no essential distinction between Betriebsegeheimnis and Geschaeftsgeheimnis,[213] except with respect to antitrust law. Section 18 of the Antitrust Act states that only important Betriebsegeheimnis (industrial secrets) are covered by the Antitrust Act. In German business and legal practice, "know-how" is often used to cover either or both Betriebsegeheimnis and Geschaeftsgeheimnis, so one must look to the context and agreement to be certain as to what is intended.

There are four requirements for trade secret protection under German law:[214]

1. The information must be secret, in the sense that the number of persons who know it is limited.
2. The information must be connected with a particular business.
3. The owner must take reasonable steps to ensure secrecy with the intent that the information remains a secret.
4. The owner has a legitimate right and interest in keeping the information secret – competitive value in maintaining secrecy is sufficient.

Thus, as in most other jurisdictions, a trade secret is confidential information held by a business that derives commercial value from secrecy, for which the owner has made reasonable efforts to maintain secrecy.

Secrecy need not be absolute. The owner of the secret may reveal it to employees and third parties, but must use commercially reasonable efforts to maintain control of it. The fact that a trade secret is susceptible to reverse engineering does not necessarily negate trade secret protection if such reverse engineering would take substantial time, expense, and effort.[215] However, where a machine is more easily susceptible to reverse engineering, and it is sold without a contractual restriction, then the secret is lost.[216]

b. Scope and Subject Matter Under Civil Law

While German civil law contains few provisions that specifically address trade secrets, it allows a plaintiff to base a civil action on criminal law. Thus, the extensive provisions of the German criminal law that address trade secrecy serve as the basis for civil actions.

These "blended actions" mainly use Section 823 of the Civil Code, which states that:

> (1) A person who, either wilfully or negligently, wrongfully interferes with or injures the life, body, health, freedom, property, or special right (sonstiges Recht) of another is bound to compensate him for any damage arising from said injury.
>
> Section 823, para. 1.[217]

213 MacLaren, Trade Secrets Throughout the World § 15:2 (2012).

214 MacLaren, Trade Secrets Throughout the World § 15:3 (2012).

215 For example, the German High Court found that a pharmaceutical was not in the public domain if an expert would need to take significant time and effort to reverse engineer the product. BGH GRUR 1980, 750 - Pankreaplex II. MacLaren, Trade Secrets Throughout the World § 15:4 (2012).

216 OLG Duesseldorf OLGR 1999, 55; MacLaren, Trade Secrets Throughout the World § 15:5 (2012).

217 Translation supplied by MacLaren, Trade Secrets Throughout the World § 15:31 (2012).

Both industrial secrets and commercial secrets protected under criminal law are treated as "special rights," which allow a plaintiff to use Section 823 of the Civil Code to bring a tort action based on a criminal statute.

Protection under civil law thus has effectively the same scope and subject matter as protection under criminal law. In addition, as noted below, typical civil law remedies (damages and injunctions) are available. However, a significant limitation on the use of civil law appears to be the lack of pre-trial discovery, as well as pleading requirements and restrictions on secrecy in civil cases. Thus, civil law cases often begin only after a criminal case is used to collect evidence because the public prosecutor does have recourse to pre-trial discovery procedures.[218]

c. Scope and Subject Matter Under Criminal Law

German criminal law contains a number of provisions that protect trade secrets. Most of these provisions are in the Act Against Unfair Competition ("UWG"). These are the most significant provisions contained in the UWG and the Criminal Code, which include the following prohibitions:

Disclosure. Disclosure by employees during the term of employment for personal gain, competitive purposes, or the benefit of a third party. UWG Section 17(1).

Industrial Espionage. Procuring or saving a trade secret without authorization for personal gain, competitive purposes, or the benefit of a third party. UWG Section 17, paragraph 2(1). "Procuring" applies to acquiring the information for the first time.[219] Acquiring the intangible secret, rather than a tangible item, such as a document or device is sufficient for procurement.[220] "Saving" makes it an offense for somebody who already has knowledge (e.g., a departing or departed employee) to download records or make photocopies to preserve or embody their knowledge.[221] The means of acquisition for the offense of industrial espionage are specified. Therefore, misappropriation by other means is not covered, but the means listed do cover a wide variety of situations. These means include:[222]

(a) acquisition through "the use of technical means, such as photocopying, copying of data files, the use of recording or listening devices in cases of oral reproduction of the secrets;"[223]

(b) "manufacture of a reproduction of the trade secret, such as the manufacture of a certain recipe or a machine which embodies the secret."[224]

(c) "the removal of a thing which embodies the secret. This may be the removal of data carriers, machines or machine elements. The substance or carrier of the embodiment are irrelevant."[225]

218 MacLaren, Trade Secrets Throughout the World § 15:31 (2012).

219 M-R. McGuire et al., Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, Germany 7 - 8 (2010).

220 Ibid.

221 Ibid.

222 Ibid.

223 Ibid.

224 Ibid.

225 Ibid.

Handling of Unlawfully Acquired Trade Secrets. Using or disclosing a trade secret obtained without authorization (through unauthorized disclosure or espionage) for personal gain, competitive purposes, or the benefit of a third party, or to damage a third party. UWG Section 17, paragraph 2(2). This provision creates liability for further use or disclosure of trade secrets by those who violate the UWG under the above provisions. It also effectively creates third party liability, but only where the third party knows or has reason to know that the trade secret was wrongly disclosed by a then-current employee pursuant to UWG Section 17, paragraph 2(1) or acquired through an act of industrial espionage pursuant to UWG Section 17, paragraph 2(2).[226] What this provision leaves out by implication is using a trade secret obtained from a departed employee (e.g. an employee hired from a competitor) who did not engage in the act of "saving" described above.[227] For purposes of this section, trade secrets retained in memory appear to be fair game.

Disclosing Technical Designs. Revealing technical designs in breach of a third party fiduciary relationship for competitive purposes or personal gain. UWG Section 18.

Attempt. Attempted inducement of a revelation of trade secrets in violation of UWG Sections 17 & 18 or making or accepting an offer to do so for competitive purposes or personal gain. UWG Sections 19 & 20.

Breach of Professional Obligations. Unauthorized disclosure or use in violation of professional obligations (e.g. doctors and lawyers), with increased penalties. Criminal Code Sections 203 & 204.

A party wishing to initiate criminal prosecution typically must apply to the public prosecutor to start proceedings (the prosecutor may, but typically does not, act on its own initiative in trade secret prosecutions). The application must be filed within 3 months of obtaining knowledge of the misappropriation. The public prosecutor may decide not to pursue the prosecution.

3. Fault

a. Standard Under Civil Law

Since civil law trade secret actions under German law typically are based on criminal statutes, they incorporate the standards of fault and intent present in such statutes.[228] (See next section.) In a civil case, a plaintiff must plead with great specificity. This requirement can be challenging, as the plaintiff may not know exactly what information or documents a defendant may possess.[229]

b. Standard Under Criminal Law

The most significant German criminal statutes discussed above generally require that the defendant intentionally disclose, use, or acquire a trade secret, without authorization, for

226 Ibid.

227 Ibid.

228 "The criminal law provisions have to be construed narrowly and require the showing of fault or intent." MacLaren, Trade Secrets Throughout the World § 15:31 (2012).

229 Hogan Lovells International LLP, Report on Trade Secrets for the European Commission, Appendix 3, at 43.

personal gain, competitive purposes, or the benefit of a third party. Third party liability requires knowledge or reason to know.[230]

4. Remedies

a. Remedies Under Civil Law

Under various provisions, most notably, Section 1 of the UWG, injunctions and damages are available. These remedies include both preliminary and permanent injunctions. Damages may include lost profits, defendant's profits, or a reasonable royalty.[231] A permanent injunction will last so long as the secret is maintained, or, if defendant acted maliciously, it may be barred from using the secret forever.[232] Destruction or return of information and materials is also available.

b. Remedies Under Criminal Law

Criminal penalties include monetary fines and prison sentences. Prison sentences are up to 2 or 3 years for most criminal provisions, with a maximum of 5 years in certain cases. Fines can range from minimal (5 Euros) to a maximum of 1.8 million Euros. Cases ending in conviction are rare and punishments are most typically monetary fines.[233]

5. Procedures

a. Emergency Action to Preserve Proof

An action is available, but plaintiffs typically find that an emergency action to preserve proof is impracticably difficult to obtain due to a high burden of proof.[234] Instead, they rely on public prosecutors bringing criminal actions to initially gather proof.[235]

b. Pre-Trial Disclosure and Discovery

Pre-trial discovery is unavailable to civil plaintiffs and they thus rely on public prosecutors to collect proof in criminal actions.[236]

c. Secrecy During Litigation

A party can apply to the court to exclude the public from proceedings. Courts generally grant such requests.

---

230 Mary-Rose McGuire et al., Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, Germany 22 - 27 (2010).

231 MacLaren, Trade Secrets Throughout the World § 15:48 (2012).

232 Ibid.

233 Hogan Lovells International LLP, Report on Trade Secrets for the European Commission, Appendix 2, at 93.

234 Hogan Lovells International LLP, Report on Trade Secrets for the European Commission, Appendix 2, at 93; MacLaren, Trade Secrets Throughout the World § 15:29 (2012).

235 Hogan Lovells International LLP, Report on Trade Secrets for the European Commission, Appendix 2, at 93; MacLaren, Trade Secrets Throughout the World § 15:29 (2012).

236 Hogan Lovells International LLP, Report on Trade Secrets for the European Commission, Appendix 2, at 93; MacLaren, Trade Secrets Throughout the World § 15:29 (2012).

6. Employee-Employer Relationships

During employment, employees have an implied duty to neither disclose nor exploit their employer's trade secrets.[237] This implied duty continues after employment, but it is more limited. First, it may not amount to a non-competition obligation.[238] Second, an employee is free to use general skills and knowledge used during employment to advance his career.[239]

Because of these limitations, the employee is generally free to use the information for his own purposes, but not to disclose it to third parties.[240] However, the employee's right to use material may be limited in certain circumstances. For example, an employee with particular fiduciary duties, or a manager in a key position may not learn information and then promptly depart to exploit it.[241] Ex-employees may not appropriate documents or use purposefully memorized material.[242] Employees may not deliberately provoke termination to put themselves in a position to use information competitively.[243]

By contrast, express, contractual obligations of confidentiality generally are enforceable.[244] However, such obligations must be reconciled with the employee's right to compete and do business on his own behalf. The duty of confidentiality must not amount to a covenant not to compete.[245] It must not hinder use of the employee's general skills and knowledge.[246] Nevertheless, agreements to keep specific, defined trade secrets confidential that do not unreasonably limit an employee's ability to work are valid.[247]

Covenants not to compete are generally and effectively enforceable only during the term of employment,[248] although express agreements are also generally unnecessary during the term of employment.[249] For a covenant not to compete to be valid after employment, it must be in writing, it must pay 50% of the most recent salary earned during employment (which is often subject to dispute), it must serve a legitimate business interest of the employer, it must be reasonable with respect to geographic scope and duration, and cannot, in any event, last longer

237 MacLaren, Trade Secrets Throughout the World § 15:45 (2012).

238 MacLaren, Trade Secrets Throughout the World § 15:45 (2012).

239 MacLaren, Trade Secrets Throughout the World § 15:45 (2012); Hogan Lovells International LLP, Report on Trade Secrets for the European Commission, Appendix 3 at 45 (2012).

240 MacLaren, Trade Secrets Throughout the World § 15:45 (2012).

241 Ibid.

242 Hogan Lovells International LLP, Report on Trade Secrets for the European Commission, Appendix 3 at 45 (2012).

243 MacLaren, Trade Secrets Throughout the World § 15:45 (2012).

244 MacLaren, Trade Secrets Throughout the World § 15:44 (2012).

245 Ibid.

246 Ibid.

247 Ibid.

248 Hogan Lovells International LLP, Report on Trade Secrets for the European Commission, Appendix 3, at 45 (2012).

249 MacLaren, Trade Secrets Throughout the World § 15:43 (2012).

than two years.[250] These extensive restrictions lead experts to conclude that they are generally not enforceable post-employment.

Commercial covenants not to compete are regulated strictly under the competition laws. They will be invalid if not limited strictly to the scope of the trade secrets, and contain no extraneous limitations.[251] Essentially, they must amount to a specific duty not to disclose or use particular trade secrets rather than a duty not to compete.[252]

7. Data Protection and Exclusivity

Germany has implemented the standard EU approach to protection of test data for pharmaceuticals set forth in EU Directive 2001/83/EC as amended by EU Directive 2004/27/EC. This approach is known as the "8 + 2 + 1 year approach." Pharmaceutical test data submitted to government for new medicinal products and new indications or uses is protected from disclosure or use for 8 years. Once the 8 year period ends, the data can be used by generic manufacturers to prepare and apply for regulatory approval, but not market a product. This period of market exclusivity lasts 2 years. The initial applicant may receive another 1 year for new indications.

8. Complementary Legal Institutions

Germany is generally regarded as having a commercial legal system that is among the most reliable and effective for contract and property rights enforcement. On the Fraser Institute Index of Economic Freedom's component index for Legal System and Property Rights, it receives a score of 8.28 out of 10, which ranks it 18th in the world.[253]

9. Technology Transfer

German law does not require foreign direct investors to transfer know-how. It does, however, restrict licenses of important trade secrets from imposing restrictions unrelated to the secret under competition law.[254]

250 Ibid.

251 MacLaren, Trade Secrets Throughout the World § 15:50 (2012).

252 See ibid.

253 Fraser Institute, Economic Freedom of the World 2012 Annual Report at 77 (2012).

254 MacLaren, Trade Secrets Throughout the World § 15:50 (2012).

India

1. Overview

Indian law has foundations in British statutes and common law because of its former status as part of the British Empire. English common law thus has an important influence on Indian law. Because of this legal heritage, India's trade secrecy law resembles UK trade secrecy law in many important respects. At the same time, India's law of trade secrecy includes its own body of decisions.

In any event, Indian trade secret law appears to be underdeveloped. Although trade secret protection is almost exclusively pursuant to the common law, one expert notes that "there is a paucity of case law on the subject of trade secrets."[255] Another expert states that "Trade Secrets seems to be a neglected field in India, as there is no enactment or policy framework for the protection of trade secrets."[256] However, as of November 2012, there was a report that the Indian government was considering trade secret legislation.[257]

Experts note that damages are apparently hard to obtain, a least in contested cases: "The courts have awarded damages but primarily in ex parte case where the defendants have chosen not to contest or even participate. In the cases which are contested, the courts have insisted upon to prove the damages suffered to quantify the claimed damage or avoid such damages. … there are hardly any cases in India post trial where damages have been quantified or awarded or the order of delivery up have been passed. Most of the cases are concluded either ex parte or by way of settlement arrived at between the parties."[258]

One expert report made the following recommendations for reform of India's trade secret laws:[259]

(1) Legislation: "It may be further desirable confidential information or trade secrets may also be dealt with by the respective intellectual property legislations such as the ones relating to Trade Marks, Copyright, Industrial Design and Patents so that they may be considered as allied rights protected in the same manner as in other intellectual property." "It is also desirable that the definition of Article 39.2 of TRIPS should be incorporated in the respective legislations since it is comprehensive and addresses relevant factors."

(2) Statutory Damages: "Quite often, it may be difficult to prove actual damage and it may be desirable to incorporate the concept of "statutory damage" in cases of breach of all kinds of intellectual property rights including trade secrets and breach of confidence."

(3) Summary Adjudication: "Considering the commercial significance and the urgency of adjudication of such matters, it may also be advisable to have a summary procedure for

255 MacLaren, Trade Secrets Throughout the World § 19:2 (2012).

256 Ramesh K. Vaidyanathan, Trade Secrets and Confidential Information, Advaya Legal Law Firm Website (September 2010), http://www.advayalegal.com/trade-secrets-confidential-information.html.

257 Subodh Ghildiyal, Govt working on norms to protect trade secrets, The Times of India (29 November 2012), http://timesofindia.indiatimes.com/business/india-business/Govt-working-on-norms-to-protect-trade-secrets/articleshow/17409936.cms.

258 Hermant Singh, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, India 6 (2010).

259 Hermant Singh, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, India 10 (2010).

adjudication of such cases. Though the Supreme Court of India has taken a stand in several cases recently that all intellectual property cases should be tried and concluded within four months, the said mandate remains more on paper than in practice."

2. Scope and Subject Matter

a. Definitions

India's statutory law contains no general definition of trade secrets. Rather, it defines trade secrets through common law, looking to English case law, particularly *Saltman Engineering Co. v. Campbell Engineering Co. Ltd.*,[260] which is a relatively early modern trade secret case that is a key precedent for trade secret protection in several common law countries.

As one authority observes, "there is a paucity of case law on the subject of trade secrets" in India.[261] Nevertheless, India, like other common law countries following *Saltman* and other related precedent, defines trade secrets as follows. A trade secret is information that:

(1) Has a confidential quality, and the owner has attempted to limit dissemination;
(2) Was disclosed to the defendant under confidential circumstances; and
(3) Defendant has used or disclosed the information (or threatens to do so) to the detriment of the owner.[262]

b. Scope and Subject Matter Under Civil Law

Indian courts interpret the subject matter of trade secret law broadly, similarly to many common law countries, but appear to adhere to the traditional, relationship-based view of trade secrecy. Trade secrecy covers both confidential business information and technical information.[263] The information that is the subject of trade secrecy must not be in the public domain. Secrecy need not be absolute, but dissemination must be limited to parties with some obligation to keep the information secret.[264]

Notably, Indian courts appear to follow the traditional requirement from *Coco v. A.N. Clark*[265] and other English cases that the information must be communicated under conditions that create an obligation of confidentiality. As discussed in this paper's summaries of UK law, this requirement may suppose that there must be some relationship between the parties. However, as also discussed in summaries of UK and Australian law, those jurisdictions appear to have evolved away from this requirement. Unlike these countries, but like New Zealand,

260 [1948] 65 RPC 203.

261 MacLaren, Trade Secrets Throughout the World § 19:2 (2012).

262 See Hemant Singh, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, India 6 (2010) (citing and analysing Escorts Construction v. Action Construction, 1999 PTC 36 (Del) among other cases); MacLaren, Trade Secrets Throughout the World § 19:3 – 19:4; 19:9 (2012) (citing and analysing Konrad Wiedemann GmbH v. Standard Castings Pvt. Ltd., [1985](10) IPLR 243; AIA Engineering Pvt. Ltd. v. Bharat Dand and Ors., AIR 2007 Gujarat (NOC) 1456; AIA Engineering Pvt. Ltd. v. Bharat Dand and Ors., AIR 2007 Gujarat (NOC) 1456; Mr. Diljeet Titus, Advocate v. Mr. Alfred A. Adebare and Ors., 2006 (32) PTC 609 (Del); American Express Bank Ltd. v. Priya Puri, (2006) IIILLJ 540 Del.; Bombay Dyeing and Manufacturing Co. Ltd. v. Mehar Karan Singh, 2010 (112) BomLR3759.).

263 MacLaren, Trade Secrets Throughout the Word §§ 19:3 – 19:4 (2012) (citing various cases).

264 Ibid.

265 Coco v. A.N. Clark Eng'rs Ltd., [1969] RPC 41; AB Consol. Ltd. v. Europe Strength Food Co. Pty. Ltd., [1978] 2 NZLR 515.

India appears to continue to adhere to this traditional requirement.[266] As one authority observes, "[t]rade secrets are protected in India either through contract law or through the equitable doctrine of breach of confidentiality."[267]

Thus, India appears to maintain the relationship-based view of trade secret infringement. Courts will thus look to a breach of duty, rather than misappropriation (or breach of a broadly implied duty) via surveillance or trespass. (Of course, Indian courts could evolve the doctrine to cover misappropriation by imposing a constructive duty of confidentiality as courts in England and Australia have done, but there is no indication that they have done so yet.)

Courts also will likely impose a duty on a third party that receives information as a result of breach of duty by another, at least if the third party does so knowingly.[268]

c. Scope and Subject Matter Under Criminal Law

There are no criminal statutes in India generally applicable to trade secrets.

3. Fault

a. Standard Under Civil Law

Trade secrecy law in India does not frame the cause of action for trade secret in terms of fault, such as through intentional or negligent disclosure. Rather, as discussed earlier, the offense is in using or disclosing the information in breach of a duty not to do so, regardless of whether the using or disclosing party intends to breach the duty or harm the claimant. This is particularly the case since India apparently maintains the relationship-based view of trade secrecy protection.

b. Criminal Law

There are no criminal statutes in India generally applicable to trade secrets.

4. Remedies

a. Civil Law

The following remedies are available:

- Injunctive relief, both interlocutory and permanent, including ex parte injunctions and injunctions to eliminate the defendant's wrongful head start.[269]
- Seizure and destruction of infringing materials pursuant to an order for delivery up.[270]

266 See Hemant Singh, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, India 5 (2010), which states that a trade secret claim requires "establishing that the information is not public knowledge and has been passed on to the defendant under the expressed or implied term of confidentiality and the said information have been apparently used is "Springboard" by the defendant to jump into the business field to the detriment of the plaintiff." (emphasis added).

267 MacLaren, Trade Secrets Throughout the Word § 19:8 (2012).

268 MacLaren, Trade Secrets Throughout the Word § 19:3 (2012) (quoting dicta in AIA Engineering Pvt. Ltd. v. Bharat Dand and Ors., AIR 2007 Gujarat (NOC) 1456).

269 MacLaren, Trade Secrets Throughout the Word, § 19:10 (2012); Hemant Singh, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, India 6 (2010).

270 MacLaren, Trade Secrets Throughout the Word, § 19:10 (2012).

- Monetary relief, either in the form of compensatory damages or recovery of defendant's profits.[271]

Expert opinion notes that damages are rarely awarded in practice:

> The plaintiff is also entitled along with injunctive relief to an order of delivery up i.e. the products manufactured by defendant by use of the confidential information must be delivered back to the plaintiff. However, there are hardly any cases in India post trial where damages have been quantified or awarded or the order of delivery up have been passed. Most of the cases are concluded either ex parte or by way of settlement arrived at between the parties.[272]

b. Criminal Law

There are no criminal statutes in India generally applicable to trade secrets.

5. Procedures

a. Emergency Action to Preserve Proof

In India, as in the UK, an ex parte procedure known as an Anton Piller Order is potentially available to plaintiffs seeking to preserve proof.[273] The procedure allows the plaintiff to apply directly to the court without informing the potential defendant. If granted, the plaintiff may search the defendant's premises and seize documents. The order allowing this procedure may be no more broad than is necessary to preserve the relevant evidence. An Anton Piller Order is granted at the discretion of the court upon a showing that it is necessary to preserve evidence. As discussed in this paper's summary of UK law, Anton Piller orders have proven to be controversial in some cases.

b. Pre-Trial Discovery

In India, pre-trial discovery is available but generally limited to documentary evidence under the supervision of the court.[274]

c. Secrecy During Litigation

In India, procedures to safeguard the secrecy of plaintiff's confidential information are available during trade secret litigation. The plaintiff can obtain closed or "in camera" hearings for both pre-trial procedures and the trial.[275] They also may obtain protection from the opposing party, limiting access to particular information or access to counsel or certain experts or professionals on the case.[276]

---

271 MacLaren, Trade Secrets Throughout the Word, § 19:10 (2012).

272 H. Singh, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, India 6 (2010).

273 MacLaren, Trade Secrets Throughout the Word, § 19:10 (2012); Hemant Singh, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, India 5 (2010).

274 Order XI of the Code of Civil Procedure of 1908.

275 MacLaren, Trade Secrets Throughout the Word, § 19:13 (2012); Hemant Singh, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, India 7 (2010).

276 MacLaren, Trade Secrets Throughout the Word, § 19:13 (2012); Hemant Singh, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, India 7 (2010).

6. Employee-Employer Relationships

Pursuant to Indian law, "trade secrets are protected, irrespective of contract, against misuse by employees or ex-employees, subcontractors or ex-subcontractors, licensees or ex-licensees. These cases state that the law does not, in this case, depend upon any implied contract but on the broad principles of equity that he who has received information in confidence shall not take unfair advantage of it."[277] However, Indian law also protects an employee's ability to earn a living after leaving an employer.[278] Indian courts will not prohibit an employee from using general skills and knowledge retained in memory.[279]

Non-competition agreements for both employees and businesses are generally not valid, unless the sale of a business is involved.[280]

7. Data Exclusivity and Data Protection

India provides no protection or exclusivity for data submitted for regulatory approval of pharmaceuticals.[281] It provides three years of data exclusivity for new agricultural chemicals.[282]

8. Complementary Legal Institutions

On the Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, India receives a score of 6.37 out of 10, which ranks it 63rd in the world.[283] It scores particularly low on legal enforcement of contracts (2.59 out of 10).

9. Technology Transfer

Inbound technology agreements are regulated, but much less than in the past, when trade secret licenses were required to be freely sub-licensable in India.[284] Nevertheless, registration and some substantive review are still required, unless certain requirements for automatic approval met.[285]

---

277 MacLaren, Trade Secrets Throughout the Word, § 19:9 (2012).

278 Ibid § 19:4 (citing Bombay Dyeing and Manufacturing Co. Ltd. v. Mehar Karan Singh, 2010 (112) BomLR3759.

279 Ibid.

280 MacLaren, Trade Secrets Throughout the Word, § 19:8 (2012).

281 See Prashant Reddy, The Data Exclusivity Debate in India: Time for a rethink? (2013), available at http://ssrn.com/abstract=2231027.

282 46th Report on the "Pesticide Management Bill, 2008," Department Related Parliamentary Standing Committee on Agriculture (2008).

283 Fraser Institute, Economic Freedom of the World 2012 Annual Report at 88 (2012).

284 MacLaren, Trade Secrets Throughout the Word, § 19:11 (2012).

285 MacLaren, Trade Secrets Throughout the Word, § 19:11 (2012).

Israel

1. Overview

The Israeli law of trade secrets is governed by the Commercial Torts Law of 1999. The Commercial Torts Law is a civil law statute that provides substantial protection for trade secrets. It builds upon and is accompanied by an extensive body of case law built on the principles of English law. Israel does not have a criminal law broadly protecting trade secrets. Commentators have described Israel's civil protection of trade secrets as broad and affording adequate protection to trade secret owners,[286] with the courts granting a broad definition with a wide and varied subject matter.[287] The law includes a full set of remedies, including a statutory damages provision.

2. Scope and Subject Matter

a. Definitions

The Commercial Torts Law defines trade secrets as: "Commercial information of every kind, which is not public knowledge or which cannot readily and legally be discovered by the public, the secrecy of which grants its owner an advantage over his competitors, provided that its owner takes reasonable steps to protect its secrecy."[288] Israeli law does not distinguish between technical information and confidential business information, and courts have protected a wide variety of secrets.[289] Thus, requirements common to many countries are applicable: the information must be commercial information, broadly understood; it must actually be secret; it must derive value from being secret; and the owner must take reasonable steps to safeguard secrecy.

b. Scope and Subject Matter Under Civil Law

As noted above, the subject matter of trade secret protection in Israel is broad. The law does not distinguish between technical information and confidential business information – all commercial information that confers a business advantage is protectable, provided other requirements are met.[290] Information must not be in the public domain, but absolute secrecy is not required.[291]

There are some restrictions on the scope of trade secrets. Reverse engineering is permitted.[292] Several cases have limited protection of customer lists – they must contain more

286 Tal Band & Ilan Miller, Question Q215: Protection of Trade Secrets Through IPR and Unfair Competition Law, AIPPI Report on Israel, 9 (2010): https://www.aippi.org/download/commitees/215/GR215israel.pdf.

287 MacLaren, Trade Secrets Throughout the World, § 21.4 (2012).

288 Commercial Torts Law, § 5, Israel - Unfair Competition (Commercial Torts). World Intellectual Property Organization, Law, 19/04/1999 -5759(il012), Available at: http://www.wipo.int/clea/docs_new/pdf/en/il/il012en.pdf.

289 MacLaren, Trade Secrets Throughout the World, § 21.4 (2012).

290 MacLaren, Trade Secrets Throughout the World, § 21.4 (2012).

291 Ibid.

292 Commercial Torts Law § 6.

than mere names, and must either include confidential details about customers or must be acquired with some difficulty from non-public sources.[293]

The Commercial Torts Law contains certain express exemptions from trade secret protection. Section 7 states:[294]

7. (a) A person shall not be liable for misappropriation of a trade secret if one of the following applies:

(1) The knowledge latent in the trade secret came into his possession in the course of his employment with the owner of the trade secret and such knowledge became part of his general professional skills;

(2) Use of the trade secret is justified as a matter of public policy.

(b) Should a person make use of a trade secret as set out in paragraph (a)(2) and gain a benefit as a result of such, the court may, if it sees fit in the circumstances of the case, order such person to return the benefit in whole or in part to the owner of the secret.

Particularly notable about this exemption is the fact that Israeli law, like the law of the UK and other countries, exempts from trade secret protection information that becomes part of the general skills and knowledge of employees.

c. Scope and Subject Matter Under Criminal Law

There are no provisions of criminal law generally applicable to trade secret theft. The Penal Law of 1977 does protect a limited category of confidential information—information related to state security—which includes a wide variety of confidential information, including trade secrets that are owned by either the state or an individual and held by the state.[295] The criminal law also prohibits disclosure of confidential information by professionals such as doctors and lawyers.[296] However, only theft of tangible items, and not information, is treated as theft.[297]

3. Fault

a. Standard Under Civil Law

Israeli trade secret law prohibits misappropriation of another's trade secret. Section 6 of the commercial torts law defines misappropriation as follows:[298]

---

293 MacLaren, Trade Secrets Throughout the World, § 21.4 (2012) (citing C.F. 512–90 (District Court) Kibbutz Negba v. Almagor Dinim Mehozi, vol. 26, p.298 and C.F. 4571/06 (Regional Labour Court) Alias Reuven and Eti Reuven v. Misochnick Inga (as yet unpublished, decision of 12.11.08), http://www.nevo.co.il/Psika_word/avoda/aa06004571-107.doc.

294 Commercial Torts Law, § 7, Israel - Unfair Competition (Commercial Torts). World Intellectual Property Organization, Law, 19/04/1999 -5759(il012), Available at: http://www.wipo.int/clea/docs_new/pdf/en/il/il012en.pdf.

295 Section 91 of the Penal Law.

296 Section 496 of the Penal Law.

297 MacLaren, Trade Secrets Throughout the World, § 21.5 (2012) (citing Katz v. The State of Israel, PD 30(3) 673; Mor v. The State of Israel, PM (1981) 468).

298 Commercial Torts Law, § 6, Israel - Unfair Competition (Commercial Torts). World Intellectual Property Organization, Law, 19/04/1999 -5759(il012), Available at: http://www.wipo.int/clea/docs_new/pdf/en/il/il012en.pdf.

(1) The taking by illegal means of a trade secret without its owner's consent; for this purpose it shall make no difference whether the secret was taken from its owner or from another person in possession of the trade secret;

(2) Use of a trade secret without its owner's consent, the use being contrary to a contractual or fiduciary obligation imposed upon the user in favour of the owner of the secret;

(3) The receiving of a trade secret or use of it without its owner's consent, the receiver or user knowing, or it being obvious at the time of receipt or use, that the secret was transferred to such person in a manner prohibited by paragraphs (1) or (2) or that the secret was transferred to any other person in such prohibited manner prior to reaching the present receiver or user.

In practice, it appears that the requirement that the taking be unlawful or illegal is less restrictive than the specific language indicates. As one authority notes "the mere taking of a trade secret will give rise to a cause of action."[299] This broad liability may stem from the fact that Israel's law takes a unique route to determining fault in trade secret cases. Section 10 of the Commercial Torts Act, in essence, "adopts the copyright presumption of 'similarity + access = infringement.'"[300] Thus, a defendant that has access to a trade secret and uses information that is the same or essentially similar to the trade secret "will be presumed to have used a trade secret belonging to the plaintiff."[301]

Moreover, an authority further opines that the law prohibits unauthorized disclosure, although it is not expressly addressed in the text of the Act. "Even though the Law does not expressly include the term "disclosure" as a prohibited act, we believe that reference therein to the term "use" includes "disclosure", as such former term is defined in the Law as including "the transfer to another person"."[302]

Thus, the law prohibits (1) unauthorized taking of a trade secret; (2) unauthorized use or disclosure in breach of a contractual or fiduciary duty; or (3) receipt of the trade secret with knowledge or reason to know that it was in violation of the latter two prohibitions.

Israeli law limits the liability of innocent recipients of trade secrets. Under Section 8 of the Commercial Torts Law, a person is not liable for receiving or using a trade secret, if he purchased and received the trade secret in good faith and for consideration. Nevertheless, that Section still allows the court to impose liability to ensure that justice is done between the parties. If the court does so, it may exempt the person being held liable from the remedies

299 Tal Band & Ilan Miller, Question Q215: Protection of Trade Secrets Through IPR and Unfair Competition Law, AIPPI Report on Israel, 5 (2010): https://www.aippi.org/download/commitees/215/GR215israel.pdf.

300 Ibid.

301 Commercial Torts Law, § 10, Israel - Unfair Competition (Commercial Torts). World Intellectual Property Organization, Law, 19/04/1999 -5759(il012), Available at: http://www.wipo.int/clea/docs_new/pdf/en/il/il012en.pdf The full text reads:

10. The defendant will be presumed to have used a trade secret belonging to the plaintiff if the following apply:
(1) The trade secret was known to the defendant or he had access to it;
(2) The information which the defendant was using is essentially similar to the information that is the subject of the trade secret.

302 Tal Band & Ilan Miller, Question Q215: Protection of Trade Secrets Through IPR and Unfair Competition Law, AIPPI Report on Israel, 5 (2010)

available to the owner of the secret, in whole or in part. "The explanatory notes to the proposed law provide that, in such situation, the court may grant injunctive relief for a limited period or may order for the royalties to be divided between the good faith purchaser and the trade secret owner."[303]

b. Standard Under Criminal Law

The limited criminal law provisions regarding trade secrets under Israeli law require a showing of intent.[304]

4. Remedies

a. Remedies Under Civil Law

Israeli law provides a wide array of remedies. These remedies are available:

- Both preliminary and permanent injunctions;[305]
- Compensatory damages, including lost profits;[306]
- An accounting of defendant's profits;[307]
- Statutory damages of up to NIS 100,000 per tortious act, regardless of actual damages;[308]
- Destruction of goods.[309]

The availability of statutory damages is notable as a remedy that is not common elsewhere.

b. Remedies Under Criminal Law

Not applicable.

5. Procedures

a. Emergency Action to Preserve Proof

Section 16 of the Commercial Torts Law expressly provides an action for seizure and preservation of evidence. Upon application of the plaintiff, the court will appoint a third party called a "temporary receiver" to search the premises of defendants and third parties with relevant evidence.[310] The receiver is empowered to seize evidence and allegedly infringing goods. Pursuant to Section 17, the court may grant such an order ex parte if there is a

303 Tal Band & Ilan Miller, Question Q215: Protection of Trade Secrets Through IPR and Unfair Competition Law, AIPPI Report on Israel, 5 (2010)

304 MacLaren, Trade Secrets Throughout the World § 21.5 (2012).

305 Civil Procedure Regulations 5744-1984.

306 MacLaren, Trade Secrets Throughout the World § 21.13 (2012).

307 MacLaren, Trade Secrets Throughout the World § 21.13 (2012).

308 Commercial Torts Law § 13.

309 Commercial Torts Law § 21.

310 Commercial Torts Law § 16.

reasonable suspicion that delay will prejudice the party requesting the order or result in the destruction of evidence.[311]

b. Pre-Trial Disclosure and Discovery

In Israel, "[t]he methods for pre-trial discovery are: (a) general orders requiring the disclosure of relevant documents; (b) orders for disclosure of specific documents; (c) requests to admit facts or documents; and (d) questionnaires (interrogatories)."[312] Generally, depositions are not available.[313]

c. Secrecy During Litigation

Section 23 of the Commercial Torts Law contains a provision expressly empowering the court to issue orders prohibiting disclosure of trade secrets revealed during litigation. Notwithstanding the constitutional principle of open court proceedings, courts may hear cases in camera to protect a trade secret pursuant to Section 68(b)(8) of the Courts Law.[314] Such protections are available during pre-trial discovery as well as during trial.[315]

6. Employee-Employer Relationships

Employees have a duty not to disclose or use trade secrets whether subject to an express agreement or not.[316] This duty continues after employment has ended.[317] However, this duty is limited in a number of ways. First, Section 7(1) of the Commercial Torts Law says that "a person shall not be liable for misappropriation of a trade secret if . . . [t]he knowledge latent in the trade secret came into his possession in the course of his employment with the owner of the trade secret and such knowledge became part of his general professional skills."[318] Thus, in Israel as in many countries, there is a policy that favors employees' freedom to practice their occupation. Knowledge that becomes part of general professional skills is not protected as a trade secret.

Contractual restrictions on competition, including covenants not to compete or agreements that expressly protect information exempted pursuant to Section 7(1), are enforceable, but only if reasonable. They are subject to a two-part test: (1) the restrictions must be no broader than reasonably necessary to protect the legitimate interests of the parties; and (2) the restrictions should not harm the public. Reasonableness of a non–competition clause is a function of the length and geographic breadth of the clause.[319] "[I]n cases involving the sale of trade secrets or know-how the courts are likely to allow restrictions that are wider in scope

311 Commercial Torts Law § 17.

312 Eric Sherby, A Primer on Commercial Litigation in Israel, 10 (2004),: http://www.sherby.co.il/Primer.pdf.

313 Ibid.

314 Tal Band & Ilan Miller, Question Q215: Protection of Trade Secrets Through IPR and Unfair Competition Law, AIPPI Report on Israel, 6-7 (2010).

315 Ibid.

316 Tal Band & Ilan Miller, Question Q215: Protection of Trade Secrets Through IPR and Unfair Competition Law, AIPPI Report on Israel, 8 (2010).

317 Ibid.

318 Commercial Torts Law, § 7(1), Israel - Unfair Competition (Commercial Torts). World Intellectual Property Organization, Law, 19/04/1999 -5759(il012), Available at: http://www.wipo.int/clea/docs_new/pdf/en/il/il012en.pdf.

319 MacLaren, Trade Secrets Throughout the World § 21.8 (2012).

than is the case with employer-employee covenants, and they are less likely to intervene in the contractual arrangement between the parties."[320] In the absence of an express non-competition clause, the Supreme Court of Israel has said that courts can only enjoin ex-employees from disclosing the employer's trade secrets, but not from working for a competing business.[321] However, there is some doubt on this point.[322]

7. Data Protection and Exclusivity

In April 2005, Israel introduced its first data exclusivity law protecting pharmaceutical test data. Israel amended the statute in 2011. The World Trade Organization's recent Trade Policy Review of Israel described the regime as follows:

> Under this regime, protection is available for test data regarding drugs with new active ingredients, not merely new indications. Generic pharmaceutical companies may file applications based on bioequivalence during the exclusivity period, but marketing approval for such pharmaceuticals will only be granted after the protection for the originator's test data has expired. The protection period, as amended in 2011, provides for a period of exclusivity of up to 6.5 years, calculated from the first product registration of the pharmaceutical in a number of developed reference countries including the United States and the European Union. This linkage of the term of protection to the reference countries is intended to encourage early launch of protected innovative pharmaceutical products in Israel. Under the amended regime, marketing approval for pharmaceutical products in Israel should be granted within 12 months of an application. This means that following a timely application for marketing approval, the effective duration of protection in Israel can last for five years. Neither registration nor marketing approval is required in Israel for pharmaceuticals that are exported.[323]

Israeli authorities have tentatively reported that agricultural chemical test data are accorded a period of exclusivity of 10 years. This is subject to confirmation via published sources (pending).

8. Complementary Legal Institutions

On the Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, Israel receives a score of 6.96 out of 10, which ranks it 38th in the world.[324] It receives middling scores on most sub-components, but receives a relatively low score with respect to enforcement of contract (3.46 out of 10) and a relatively high score with respect to judicial independence (8.63 out of 10).

9. Technology Transfer

Israel does not subject foreign investors to technology transfer requirements, joint venture technology contribution requirements, or license registration requirements.

---

320 MacLaren, Trade Secrets Throughout the World § 21.7 (2012).

321 MacLaren, Trade Secrets Throughout the World § 21.8 (2012).

322 Ibid.

323 Trade Policy Review Body – Report by the Secretariat – Israel, WT/TPR/S/272, 52 (25 September 2012).

324 Fraser Institute, Economic Freedom of the World 2012 Annual Report at 92 (2012).

Italy

1. Overview

Italy protects trade secrets under both civil law and criminal law. Civil law protection has been codified by, essentially, incorporating Articles 39(2) and 39(3) of TRIPS into the Italian Code of Industrial Property. Criminal protection is more limited and specific, applying to employees[325] or to the theft or unauthorized use of documents or other media.[326]

Trade secret protection is relatively broad, but experience with comprehensive trade secret protection is relatively limited. Before implementing TRIPS, trade secret protection was limited to various scattered, specific provisions of the Civil and Criminal Codes. A commentator noted the recent vintage of trade secret law as a challenge:

> Notwithstanding the fact that our country has implemented the TRIPs agreement and the EC Enforcement Directive, since the provisions recognizing the protection of trade secrets as an IP right have been introduced in our IP Code only recently, there is not yet a reliable case law allowing a stable interpretation of the rules.[327]

2. Scope and Subject Matter

a. Definitions

Italy adopted Articles 39(2) and 39(3) of TRIPS "verbatim"[328] into the Italian Code of Industrial Property ("IPC").[329] The provisions are set forth in Articles 98 of the IPC. For reference, the original English text of TRIPS Article 39(2) is set forth here:

> 2. Natural and legal persons shall have 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 so long as such information:
>
> (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.
>
> 3. 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

325 Article 623 of the Italian Criminal Code.

326 Article 621 of the Italian Criminal Code.

327 Lamberto Liuzzo et al., Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, Italy, 11 (2010).

328 Ibid.

329 Legislative Decree No. 30 of 10 February 2005 and amended by Legislative Decree No. 131 of 13 August 2010, under the header "Secret information".

> necessary to protect the public, or unless steps are taken to ensure that the data are protected against unfair commercial use.

b. Scope and Subject Matter Under Civil Law

The subject matter protected by Italian law as trade secrets is broad. It protects both confidential business information and technical information as trade secrets.[330] Trade secret infringement is defined in Article 99 of the IPC. It states:

> [T]he legitimate owner of the business information and expertise set forth in Article 98 is entitled to prohibit third parties, absent his consent, from acquiring, disclosing to others or using, abusively, such information and expertise, except for cases where they have been achieved autonomously by the third party in question.[331]

This Article "clarifies that secret information is not protected per se by the law." [332] Rather, all of the requirements of Article 98 must be met: The information must indeed be secret; it must derive value from secrecy; and the owner must take reasonable steps to safeguard secrecy. Infringement occurs only if "the information in question has been acquired by a third party abusively, i.e. by taking the information out of the exclusive control of the legitimate owner without his consent."[333] As the text of Article 98 states, the offense includes acquiring, using, or disclosing the information without the owner's consent. The right in trade secrets, however, is not exclusive, because independent development is a defence.

Because trade secrets are treated as intellectual property rights, good faith, unknowing receipt of secrets would appear not to be a defence under the law,[334] but one recent commentator noted that in practice it appears to be as follows:

> [F]or those cases where secret information is misappropriated and passed over by the infringer to a third party who acquires it in good faith, Italian commentators have long excluded the liability of the innocent recipient. In this regard, the Courts also tended to apply traditional unfair competition doctrines (instead of the purely proprietary regime implied by the IPC), excluding liability where the plaintiff is not able to demonstrate that the defendant-receiver was aware of the misappropriation. This seems to be confirmed by the recent amendments to Article 99 IPC, which clarify that infringement actions can be brought only against "abusive" appropriation of the secret information.[335]
>
> In addition, Article 2598 no. 3 of the Italian Civil Code, which addresses acts of unfair competition in general terms, may also apply to trade secret

330 Hogan Lovells International LLP, Report on Trade Secrets for the European Commission, Appendix 2, at 156 (2012).

331 Article 99 IPC, as amended by Legislative Decree No. 131 of 13 August 2010.

332 Hogan Lovells International LLP, Report on Trade Secrets for the European Commission, Appendix 2, at 156 (2012).

333 Hogan Lovells International LLP, Report on Trade Secrets for the European Commission, Appendix 2, at 156 (2012).

334 Lamberto Liuzzo, et al., Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, Italy, 7 (2010).

335 Hogan Lovells International LLP, Report on Trade Secrets for the European Commission, Appendix 3, 51 (2012).

misappropriation. Article 2598 is likely to be invoked where the slightly stricter definition of trade secrecy set forth in Articles 98 and 99 of the IPC does not apply, "e.g., the information is not subject to specific measure to keep it secret but has an intrinsic confidential nature and is such as to give a technical/economic information advantage to its owner."[336] For purposes of this study, and the index it constructs, the applicability of Article 2598 appears to broaden the availability of trade secret protection in Italy, thus making the measure both more typical and more stringent than it might otherwise be.

c. Scope and Subject Matter Under Criminal Law

Italy protects trade secrets under criminal law, but the scope is narrower than under civil law. In essence, only employees are potentially liable for trade secret theft. The relevant provisions are:

- Penalties of up to 1 year in jail or a fine of 516 Euros for use or disclosure of a secret obtained during the course of employment.[337]
- Penalties of up to 2 years in jail for use or disclosure of a secret regarding scientific discoveries, inventions, or industrial applications learned during the course of employment.[338]

In addition, in a provision aimed at trade secrecy the law punishes theft or unauthorized use of documents or other media or device containing data information or programs with penalties of up to 3 years in jail or a fine of up to 1 032 Euros.[339] However, this provision does not protect the underlying information, and therefore does not cover, for example, information photographed, observed, memorized or verbally communicated.

These provisions are thus limited to theft of physical media or disclosure or use of trade secrets by employees. "Most claims for trade secret infringement are brought under Articles 98 and 99 IPC, given the broader scope of protection granted by those provisions and the wide array of available civil remedies."[340]

3. Fault

a. Standard Under Civil Law

Italy treats trade secrets as property. Provided they meet the definition of Article 98 of the IPC, the unauthorized use, disclosure or acquisition of them violates the law. This standard of fault appears contrast to countries that only find fault where there has been a violation of duty or the circumstances of acquisition are improper. However, in 2010, Article 99 of the IPC was amended in to specify that appropriation must be "abusive," a term which is not otherwise

336 Baker & McKenzie, Study on Trade Secrets and Confidential Business Information in the Internal Market, Appendix 6, 285 (2013). See also ibid at 292 – 297 (describing cases).

337 Article 622 of the Italian Criminal Code.

338 Article 623 of the Italian Criminal Code.

339 Article 621 of the Italian Criminal Code.

340 Hogan Lovells International LLP, Report on Trade Secrets for the European Commission, Appendix 2, at 158 (2012).

defined under the law. At the very least, this provision appears to exempt from liability parties who receive trade secrets without knowledge and in good faith.[341]

b. Standard Under Criminal Law

A defendant must have intent to violate Italy's criminal trade secret laws.[342]

4. Remedies

a. Remedies Under Civil Law

A wide array of remedies for trade secrecy infringement is available in Italy:[343]

- Preliminary injunctions and temporary restraining orders.
- Compensatory damages.
- Destruction of infringing goods.

b. Remedies Under Criminal Law

See Section 2(c) above.

5. Procedures

a. Emergency Action to Preserve Proof

To preserve proof, party may obtain a preliminary search order pursuant to Articles 129-130 of the IPC. Plaintiff must show a prima facie case and that the evidence may be destroyed or unavailable later.[344] If there is a risk that proof might be altered, the search order may be available on an ex parte basis.[345] Such an order allows the petitioner to conduct a search of defendant's premises, accompanied by a bailiff and expert.

b. Pre-Trial Disclosure and Discovery

In Italy, limited pre-trial disclosure and discovery is available pursuant to Article 121(2) of the IPC. A party may request that the court order the opposing party to provide documents and other information, as well as the identity of people involved in the alleged infringement. Article 121(3) requires the court to take adequate measures to protect confidential information when issuing such orders. Such discovery "may or may not be granted at the discretion of the judge. More important, no specific enforcement tool or sanction is established against parties who refuse to comply with the orders, apart from the general negative inferences the court will likely draw in relation to parties not complying with court orders."[346]

---

341 Hogan Lovells International LLP, Report on Trade Secrets for the European Commission, Appendix 3, 51 (2012).

342 Lamberto Liuzzo, et al., Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, Italy, 7 (2010).

343 Hogan Lovells, Appendix 2, at 158 (2012).

344 Hogan Lovells International LLP, Report on Trade Secrets for the European Commission, Appendix 2, at 158 (2012).

345 Hogan Lovells International LLP, Report on Trade Secrets for the European Commission, Appendix 2, at 158 (2012).

346 Daniela Ampollini, Italy in E-Discovery and Data Privacy: A Practical Guide 132 (Catrien Noorda & Stefan Hanloser 2010).

c. Secrecy During Litigation

Protection of secrecy during litigation is incomplete. Hearings before the investigating judge are non-public, but the final hearing before the panel of Judges issuing a decision is public.[347] Such a hearing can only be closed for reasons of national security, public order, or decency.[348] The final decision must be public.[349]

6. Employee-Employer Relationships

During employment, an employee has a duty of loyalty under Article 2105 of the Civil Code. Even in the absence of an express contractual obligation, the employee has a duty not to compete or reveal the employer's trade secrets.[350] After employment, contractual obligations to keep information confidential remain in force and are enforceable.[351]

Non-competition clauses are not enforceable unless they meet the following requirements: (1) they must be limited in time—5 years for executives and 3 years for other employees; (2) they must be limited in geographic scope; (3) they must cover specific work activities; and (4) they must pay compensation no lower than 20 – 30% of monthly salary, including benefits and bonuses.[352]

7. Data Protection and Exclusivity

Italy has implemented the standard EU approach to protection of test data for pharmaceuticals set forth in EU Directive 2001/83/EC as amended by EU Directive 2004/27/EC. This approach is known as the "8 + 2 + 1 year approach." Pharmaceutical test data submitted to government for new medicinal products and new indications or uses is protected from disclosure or use for 8 years. Once the 8 year period ends, the data can be used by generic manufacturers to prepare and apply for regulatory approval, but not market a product. This period of market exclusivity lasts 2 years. The initial applicant may receive another 1 year for new indications.

8. Complementary Legal Institutions

On the Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, Italy receives a score of 5.95 out of 10, which ranks it 61st in the world.[353] It ranks relatively low with respect to judicial independence (4.99 out of 10), impartial courts (2.73 out of 10), and legal enforcement of contracts (3.18 out of 10).

9. Technology Transfer

Israel does not subject foreign investors to technology transfer requirements, joint venture technology contribution requirements, or license registration requirements.

---

347 Hogan Lovells International LLP, Report on Trade Secrets for the European Commission, Appendix 3, 49 (2012).

348 Ibid.

349 Ibid.

350 Ibid. at 53.

351 Ibid. at 53.

352 Ibid. at 53.

353 Fraser Institute, Economic Freedom of the World 2012 Annual Report at 93 (2012).

Japan

1. Overview

Japan has developed broad and increasingly strong protection for trade secrets over the past twenty years. Japan provides both comprehensive civil and criminal protection under the Unfair Competition Prevention Act. Its laws are considered strong and effective, although some of them are still relatively new. In particular, its criminal trade secret laws have been updated in 2005 and 2009.

The largest caveats with respect to Japanese trade secret law have to do with the security of information during criminal proceedings and the ease of obtaining injunctions. First, constitutional requirements in criminal proceedings mean that the proceedings and record must stay open.[354] Thus, "criminal remedies are rarely used against the acts of trade secret infringement" due to fear of publication.[355] Second, preliminary injunctions, which are crucial in trade secret cases, can be difficult to obtain. As one expert observes:

> A holder of trade secret may exercise his right to seek injunction through a normal civil trial or the filing of a motion for preliminary injunction. However, in the case of a motion for preliminary injunction, it is legally necessary in principle that there be a court hearing with the presence of the respondent. Although the proceedings for preliminary injunction are faster than a normal civil trial, it usually takes several months before a ruling is made.[356]

2. Scope and Subject Matter

a. Definitions

The Unfair Competition Prevention Act of 1993 defines trade secrets as follows: "The term 'trade secret' as used in this Act means technical or business information useful for commercial activities such as manufacturing or marketing methods that is kept secret and that is not publicly known."[357] Japanese law does not distinguish between technical information and confidential business information, and courts have protected a wide variety of secrets.[358] While absolute secrecy is not necessary, the requirement that information be "kept secret and ... not publicly known" is understood to require the trade secret owner to take reasonable steps to preserve secrecy. As one commentator observed: "Although the drafters wanted this requirement to be uniquely worded under Japanese law, they recognize that the fundamental idea of this requirement is akin to the requirement of 'reasonable efforts to maintain secrecy' under the Uniform Trade Secret Act in the US"[359] Japanese courts have thus held that

354 Kazuo Ubukata, Question Q215: Protection of Trade Secrets Through IPR and Unfair Competition Law, AIPPI Report on Japan 9 (2010).

355 Ibid.

356 Ibid at 8.

357 Art. 1(6), Unfair Competition Prevention Act (Act No. 47 of 1993) (up to the revisions of Act No. 62 of 2011 (Effective 1 December 2011)), unofficial translation available at: http://www.wipo.int/wipolex/en/text.jsp?file_id=254517.

358 MacLaren, Trade Secrets Throughout the World § 23.3 (2012) (citing Case No. 28/2 Intellectual Property, Civil, and Administrative Decisions 300 (Osaka District Court Case No. Heisei 6 (WA) 4404 and Case No. 1010 Hanrei Times 296 (Tokyo District Court Case No. Heisei 10 (WA) 15960, cases which both protected customer lists as trade secrets.).

359 MacLaren, Trade Secrets Throughout the World § 23:2 (2012).

plaintiffs have failed to meet this requirement where they failed to take sufficient steps to safeguard a secret.[360]

Thus, requirements common to many countries are applicable in Japan: the information must be commercial information, broadly understood; it must actually be secret; and the owner must take reasonable steps to safeguard secrecy.

b. Scope and Subject Matter Under Civil Law

As noted above, the subject matter of trade secret protection in Japan is broad. The law does not distinguish between technical information and confidential business information – it protects all "technical or business information useful for commercial activities," provided other requirements are met.[361] The law thus protects "information [that] can be used in commercial activities or that . . . can be used to reduce costs or improve the operational efficiency. The technical or business information includes a product design and manufacturing method, a list of customers, a sales manual, and a supplier list."[362]

As described above, information must not be publicly known, but absolute secrecy is not required. Rather, the owner must take reasonable steps to protect the information from disclosure. This does not mean that the holder of a trade secret intends subjectively to keep it secret, but that employees or outsiders can objectively see that it is kept secret. Another point is to what extent it should be kept secret. It is considered to be sufficient if information can be reasonably recognized as a secret based on the situation where it is kept."[363]

c. Scope and Subject Matter Under Criminal Law

The scope and subject matter of criminal sanctions for trade secret behaviour is generally the same as with respect to civil protection. Both technical information and confidential business information are protected.

3. Fault

a. Standard Under Civil Law

Japanese trade secret law prohibits both misappropriation of trade secrets and the misuse or wrongful disclosure of trade secrets in breach of duty. Article 2(1), subsections (iv) to (ix) of the Unfair Competition Prevention Act set forth the relevant offenses.

What many jurisdictions describe as misappropriation of trade secrets is designated in subsection (iv) of the Act as "acts of wrongful acquisition."[364] These actions include "acts of

360 Ibid at §§ 23:2 – 23.3 (describing cases where failure to establish internal security procedures for data and failing to secure non-disclosure agreements from outside experts rendered information non-secret).

361 Art. 1(6), Unfair Competition Prevention Act (Act No. 47 of 1993) (up to the revisions of Act No. 62 of 2011 (Effective 1 December 2011)), unofficial translation available at: http://www.wipo.int/wipolex/en/text.jsp?file_id=254517.

362 Kazuo Ubukata, Question Q215: Protection of Trade Secrets Through IPR and Unfair Competition Law, AIPPI Report on Japan 4 (2010).

363 Kazuo Ubukata, Question Q215: Protection of Trade Secrets Through IPR and Unfair Competition Law, AIPPI Report on Japan 4 (2010).

364 Art. 2(1)(iv), Unfair Competition Prevention Act (Act No. 47 of 1993) (up to the revisions of Act No. 62 of 2011 (Effective 1 December 2011)), unofficial translation available at: http://www.wipo.int/wipolex/en/text.jsp?file_id=254517.

acquiring a trade secret by theft, fraud, duress or other wrongful means."[365] Subsections (iv), (v) and (vi) further prohibit using or disclosing such wrongfully acquired information.[366] This prohibition on use and disclosure of wrongfully acquired information applies to: (a) the party that originally acquired the information wrongfully; (b) third parties that acquire the information that know or should know (the standard is "gross negligence") that the information was wrongfully acquired; and (c) third parties that have subsequently become aware or should have become aware (once again, the standard is "gross negligence") that the information was wrongfully acquired.[367]

Acts of wrongful acquisition are defined broadly. Not only do they include criminal or tortious acts (theft, fraud, duress), but they also include "other wrongful means."[368] "Other wrongful" acts applies broadly to commercial espionage[369] and other acts of unfair competition:

> The concept of "other wrongful method" includes not only criminal acts but also other acts that seriously violate public order or morals. Thus, unauthorized copying of another person's business information recorded on magnetic tape can be that kind of wrongful method, even if the tape is not taken from the holder's custody and thus no "theft" under the Penal Code has occurred.[370]

Such wrongful means also include "embezzlement and the unauthorized reproduction of a data storage medium containing a trade secret by a person, in breach of the duty to keep safe custody of trade secrets."[371]

---

365 Ibid.

366 Art. 2(1)(iv) – (vi) of the Unfair Competition Prevention Act are as follows:

(iv) acts of acquiring a trade secret by theft, fraud, duress or other wrongful means ((hereinafter referred to as "acts of wrongful acquisition"), or the act of using or disclosing a trade secret so acquired (including the act of disclosing such trade secret in confidence to a specific person or persons; the same shall apply hereinafter);

(v) acts of acquiring a trade secret with the knowledge that such trade secret has been acquired through acts of wrongful acquisition or without the knowledge of such matter due to gross negligence, or acts of using or disclosing a trade secret so acquired;

(vi) acts of using or disclosing a trade secret after becoming aware or not becoming (vi) aware of such matter due to gross negligence;, subsequent to its acquisition, that such trade secret was acquired through wrongful acquisition.

Art. 2(1)(iv) – (vi), Unfair Competition Prevention Act (Act No. 47 of 1993) (up to the revisions of Act No. 62 of 2011 (Effective 1 December 2011)), unofficial translation available at: http://www.wipo.int/wipolex/en/text.jsp?file_id=254517.

367 MacLaren, Trade Secrets Throughout the World § 23:10 (2012).

368 Art. 2(1)(iv), Unfair Competition Prevention Act (Act No. 47 of 1993) (up to the revisions of Act No. 62 of 2011 (Effective 1 December 2011)), unofficial translation available at: http://www.wipo.int/wipolex/en/text.jsp?file_id=254517.

369 MacLaren, Trade Secrets Throughout the World § 23:10 (2012).

370 Ibid (citing K.K. Kawachi Inquiry v. K.K. Toyo Music Instruments et al., 1281 Hanrei Jiho 129 (Tokyo District Court, Case No. Showa 53 (WA) 8769, decided 1 July 1988)).

371 Kazuo Ubukata, Question Q215: Protection of Trade Secrets Through IPR and Unfair Competition Law, AIPPI Report on Japan 3 (2010).

The Act also prohibits misuse or wrongful disclosure of trade secrets in breach of duty in Art 3(1)(vii) – (ix).[372] Such breaches include unauthorized use or disclosure "committed by officers, employees, licensees or subcontractors, and others to whom the holder of a trade secret discloses its trade secret in a confidential relationship."[373] The Act further prohibits third parties from using or disclosing such information, just as it does with respect to wrongfully acquired information. Thus, it prohibits use or disclosure by third parties that acquire the information that know or should know (the standard is "gross negligence") that the information was wrongfully disclosed; and parties that have subsequently become aware or should have become aware (once again, the standard is "gross negligence") that the information was wrongfully disclosed.[374]

The law therefore applies to third parties who have knowledge or should know that the trade secret was wrongfully acquired or disclosed. It thus excuses innocent third parties from liability when they acquire a trade secret in good faith. However, that exemption from liability ends once they become aware of the breach of trade secrecy that originally made the trade secret available: "Bad faith after acquiring the trade secret in good faith will be implied after receipt of formal notification by the trade secret holder, commencement of a law suit, or publication in a newspaper or like media that an unfair act was involved."[375]

Thus, the law prohibits (1) misappropriation of a trade secret; (2) unauthorized use or disclosure in breach of a contractual or other duty; or (3) receipt of the trade secret with knowledge or reason to know that it was in violation of the latter two prohibitions.

b. Standard Under Criminal Law

Article 21(1) of the Unfair Competition Prevention Law imposes criminal sanctions for trade secret theft. The Act sanctions both misappropriation and breach of duty. Relatively

372 Art. 2(1)(vii) – (ix) of the Unfair Competition Prevention Act are as follows:

(vii) acts of using or disclosing a trade secret, which has been disclosed by the business operator holding such a trade secret (hereinafter referred to as the "holder"), for the purpose of acquiring an illicit gain, or causing injury to such holder;

(viii) acts of acquiring a trade secret with the knowledge or, without the knowledge due to gross negligence, that there has been an improper disclosure of such trade secret (which means, in the case prescribed in the preceding item, acts of disclosing a trade secret for the purpose prescribed in said item, or acts of disclosing a trade secret in breach of a legal duty to maintain secrecy; the same shall apply hereinafter) or that such trade secret has been acquired through improper disclosure, or acts of using or disclosing a trade secret so acquired;

(ix) acts of using or disclosing an acquired trade secret after becoming aware or not being aware of such matter due to gross negligence, subsequent to its acquisition, that there has been improper disclosure of such trade secret or that such trade secret has been acquired through improper disclosure.

Art. 2(1)(vii) – (ix), Unfair Competition Prevention Act (Act No. 47 of 1993) (up to the revisions of Act No. 62 of 2011 (Effective 1 December 2011)), unofficial translation available at: http://www.wipo.int/wipolex/en/text.jsp?file_id=254517.

373 MacLaren, Trade Secrets Throughout the World § 23:10 (2012).

374 Ibid.

375 MacLaren, Trade Secrets Throughout the World § 23:10 (2012).

recent amendments to the Act in 2005 and 2009 significantly broadened and strengthened criminal trade secret law in Japan.

As it now exists, the law covers essentially the same behavior as civil trade secret law, albeit described differently. For example, Article 12(1)i covers

> a person who acquires a trade secret by an act of fraud or others (which means (i) an act of deceiving, assaulting, or intimidating a person; the same shall apply hereinafter in this Article) or an act violating control obligations (which means an act of stealing property, trespassing on a facility, making an unauthorized access [an act of unauthorized access prescribed in Article 3 of the Unauthorized Computer Access Act (Act No. 128 of 1999)], or violating the control of a trade secret maintained by its holder in any other way.[376]

These two concepts—acquisition by fraud or violation of control—appear to correspond to civil liability for wrongful acquisition. Similarly, Article 21 contains criminal sanctions for breach of duty for wrongly using or disclosing a trade secret in breach of duty just as the civil liability sections of the Act also do.

The Act's criminal sanctions specify a broad class of intentional acts as sanctionable. They cover misappropriation, breach of duty, or acquisition of a third party for the "purpose of acquiring an illicit gain or causing injury to the holder."[377] "Further, the amendment of 2009 changed that, in addition to 'use or disclosure' of business secrets, possession of the information outside of assigned business purposes and copying such information without authorization are punishable."[378] Moreover, third parties can be criminally liable if they acquire or use a trade secret that was wrongfully acquired or disclosed in breach of duty if they do so for the "purpose of acquiring an illicit gain or causing injury to the holder."[379]

Japanese criminal law with respect to trade secrets also applies extraterritorially:

> Under Article 21, (4) it is provided that the offenses prescribed in (1), (ii) or (iv) (vii) shall also apply to a person who commits said offenses outside Japan with regard to trade secrets controlled from within Japan at the time of the fraud, etc., or the act of violating control, or at the time the trade secret was disclosed by its holder.[380]

4. Remedies

a. Remedies Under Civil Law

Japanese law provides a wide array of remedies. These remedies are available pursuant to Article 3 Paragraph 1 of the Unfair Competition Prevention Law:

---

376 Art. 21(1)(i), Unfair Competition Prevention Act (Act No. 47 of 1993) (up to the revisions of Act No. 62 of 2011 (Effective 1 December 2011)), unofficial translation available at: http://www.wipo.int/wipolex/en/text.jsp?file_id=254517.

377 Ibid.

378 MacLaren, Trade Secrets Throughout the World, § 23:6 (2012).

379 Ibid.

380 MacLaren, Trade Secrets Throughout the World, § 23:6 (2012).

- Both preliminary and permanent injunctions;[381]
- Compensatory damages, including lost profits;[382]
- Alternately, damages may be based on defendant's profits or a reasonable royalty;[383]
- Destruction of goods or equipment that facilitate infringement or closure of facilities where infringement occurs.[384]

Ex parte injunctions are not available.[385]

b. Remedies Under Criminal Law

Criminal sanctions include the following:

- For individuals, up to 10 years imprisonment and/or a fine of up to ten million yen.[386]
- For a corporation, up to 300 million yen.[387]

One expert comments on the application of penalties in practise: "The prescribed penalty for crimes against property is mainly imprisonment with labour. ... The sentence is often suspended for the first-time offender. Fines are normally not imposed, but confiscation is possible."[388]

5. Procedures

a. Emergency Action to Preserve Proof

There is very limited provision in Japan for pre-trial procedures to preserve evidence. A party may move for an order to preserve evidence.[389] However, the court will not usually

381 MacLaren, Trade Secrets Throughout the World, § 23:15 (2012); Kazuo Ubukata, Question Q215: Protection of Trade Secrets Through IPR and Unfair Competition Law, AIPPI Report on Japan 8 (2010).

382 MacLaren, Trade Secrets Throughout the World, § 23:16 (2012); Kazuo Ubukata, Question Q215: Protection of Trade Secrets Through IPR and Unfair Competition Law, AIPPI Report on Japan 8 (2010).

383 MacLaren, Trade Secrets Throughout the World, § 23:16 (2012); Kazuo Ubukata, Question Q215: Protection of Trade Secrets Through IPR and Unfair Competition Law, AIPPI Report on Japan 8 (2010).

384 MacLaren, Trade Secrets Throughout the World, § 23:15 (2012); Kazuo Ubukata, Question Q215: Protection of Trade Secrets Through IPR and Unfair Competition Law, AIPPI Report on Japan 8 (2010)..

385 Kazuo Ubukata, Question Q215: Protection of Trade Secrets Through IPR and Unfair Competition Law, AIPPI Report on Japan 8 (2010).

386 MacLaren, Trade Secrets Throughout the World, § 23:7 (2012); Kazuo Ubukata, Question Q215: Protection of Trade Secrets Through IPR and Unfair Competition Law, AIPPI Report on Japan 8-9 (2010).

387 MacLaren, Trade Secrets Throughout the World, § 23:7 (2012); Kazuo Ubukata, Question Q215: Protection of Trade Secrets Through IPR and Unfair Competition Law, AIPPI Report on Japan 8-9 (2010).

388 MacLaren, Trade Secrets Throughout the World, § 23:7 (2012); Kazuo Ubukata, Question Q215: Protection of Trade Secrets Through IPR and Unfair Competition Law, AIPPI Report on Japan 8-9 (2010).

389 Tsuneo Sato, International Civil Procedure: Japan § 5.2 (2003).

order access to documents or other materials, but rather will require the party possessing the documents to preserve evidence.[390] Moreover, "an order to preserve evidence prior to the lawsuit does not entail an obligation to submit documents in many cases and a holder of relevant documents may refuse to submit them."[391]

b. Pre-Trial Disclosure and Discovery

Discovery in Japan is limited.[392] As one commenter describes it:

> While the Code of Civil Procedure does allow for the gathering of documents and making inquiries to the opposing party, judges are very conservative in issuing orders requiring the production of documents until the court is convinced that such a document is highly relevant to the proceedings. The parties do not exchange witness lists or make requests for admissions, and depositions are not permitted as a matter of right.[393]

c. Secrecy During Litigation

Japanese law contains extensive measures to protect trade secrets during civil litigation.[394] A party may refuse to testify or provide documents that contain trade secrets. Both proceedings and the trial record are protected if they contain trade secrets, allowing for limited access to the record and in camera hearings.[395] Courts will issue protective orders, and sanctions for not complying can be onerous.[396]

By contrast, "there is no system in place for preventing the publication of trade secrets to be tried in criminal proceedings, which is related to the fact that the openness of a trial is guaranteed by the Constitution."[397] This makes criminal proceedings relatively rare, as companies are reluctant to expose their secrets.[398]

6. Employee-Employer Relationships

Both express and implied obligations to protect trade secrets are enforceable against current and former employees and business partners.[399] Post-relationship implied duties generally apply:

---

390 Ibid.

391 Kazuo Ubukata, Question Q215: Protection of Trade Secrets Through IPR and Unfair Competition Law, AIPPI Report on Japan 23-24 (2010).

392 Carl F. Goodman, "Japan's New Civil Procedure Code: Has It Fostered A Rule Of Law Dispute Resolution Mechanism?", Brook. J. Int'l L. 511, 571 – 585 (2004).

393 Tsuneo Sato, International Civil Procedure: Japan § 5.2 (2003).

394 Kazuo Ubukata, Question Q215: Protection of Trade Secrets Through IPR and Unfair Competition Law, AIPPI Report on Japan 10-13 (2010).

395 Ibid.

396 Ibid at 13.

397 Kazuo Ubukata, Question Q215: Protection of Trade Secrets Through IPR and Unfair Competition Law, AIPPI Report on Japan 9 (2010).

398 Kazuo Ubukata, Question Q215: Protection of Trade Secrets Through IPR and Unfair Competition Law, AIPPI Report on Japan 9, 19 (2010).

399 Kazuo Ubukata, Question Q215: Protection of Trade Secrets Through IPR and Unfair Competition Law, AIPPI Report on Japan 17 (2010).

> Even without a specific provision in the contract, under a general employment agreement or contract, written or oral, employees or similar persons are prohibited from disclosing trade secrets of their employer or another rights holder on the basis of the fundamental principle of trust and good faith between contractual parties.[400]

Post-employment non-disclosure agreements are subject to some review to ensure they are reasonable, but they are generally enforceable. As one observer notes:

> Since the principle of the freedom of contract applies, a nondisclosure agreement like this is basically considered effective in this country. (However, if such nondisclosure obligation lasts for a long period of time after the termination of employment or the scope of the obligation is excessively wide, it may be judged to be invalid on the ground that it is against public policy.)[401]

Non-competition agreements are judged more strictly "because it may restrict these employees' freedom of job selection (Article 22 (1) of the Constitution)."[402]

> [I]n order for a non-competition obligation to be judged as effective, its imposition should be permitted only when there are legitimate interests to be protected by such prohibition, for example: the prevention of the outflow of know-how or the retention of their clients, with reasonable limitations on when (the period) and where the competition will be prohibited in order to achieve these objectives.[403]

7. Data Protection and Exclusivity

Japan provides data protection as follows:[404] For new chemical entities, it provides up to 8 years during which data submitted for regulatory approval is protected from disclosure cannot be relied upon by a third party to obtain approval. It provides 4 to 6 years of protection for certain improvements. Finally, it provides 10 years of protection for orphan drugs.

8. Complementary Legal Institutions

On the Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, Japan receives a score of 7.49 out of 10, which ranks it 28th in the world.[405] Its lowest scores are with respect to impartial courts (5.92 out of 10) and legal enforcement of contracts (5.8 out of 10).[406]

9. Technology Transfer

While Japan once had extensive technology transfer regulations affecting trade secret licensing, those regulations are largely gone. What remains are relatively common competition-related regulations.

---

400 MacLaren, Trade Secrets Throughout the World § 23:10 (2012).

401 Kazuo Ubukata, Question Q215: Protection of Trade Secrets Through IPR and Unfair Competition Law, AIPPI Report on Japan 17 (2010).

402 Ibid.

403 Ibid.

404 Tony Ellery, Neal Hansen, Pharmaceutical Lifecycle Management: Making the Most of Each and Every Brand §§ 9.5 – 9.6 (Wiley & Sons 2012).

405 Fraser Institute, Economic Freedom of the World 2012 Annual Report at 95 (2012).

406 Ibid.

Korea

1. Overview

Korea has comprehensive laws protecting trade secrets, which have been updated frequently over the past two decades. Korea provides both civil and criminal protection, a broad set of remedies, and, as of 2012, protective measures to safeguard trade secrets during litigation.[407]

Commentators observe that Korea has grown increasingly protective of trade secrets, but some parties continue to express specific concerns. As Korea has become a leader in innovation and high technology manufacturer, trade secret protection has been viewed as and treated as increasingly important.[408] However, parties have complained that test data filed to comply with regulatory requirements has leaked to competitors.[409] A 2011 Investment Climate Statement by the US Department of State observed:

> Korean laws on unfair competition and trade secrets provide a basic level of trade secret protection in Korea, but are insufficient in some instances. For example, some US firms, particularly certain manufacturers of chemicals, pet food, cosmetics, and food products, face continuing problems with government regulations requiring submission of very detailed product information, such as formula or blueprints, as part of registration or certification procedures. US firms report that, although the release of business confidential information is forbidden under Korean law, in some instances, government officials do not sufficiently protect this proprietary information, and trade secrets appear to have been made available to Korean competitors or to their trade associations.[410]

Nevertheless, the US government has also commented favourably in the past on Korea's commitment to address this issue in the US – Korea Free Trade Agreement concluded in 2007.[411]

2. Scope and Subject Matter

The primary source of law concerning trade secret protection in Korea is the Unfair Competition Prevention law and Trade Secrets Protection Act (the Trade Secrets Act).

a. Definitions

The Trade Secrets Act contains a definition of trade secrets that is substantially identical to the one contained in TRIPS Article 39(2). The definition is set forth in Article 1, Paragraph 2, of the Trade Secrets Act:

---

407 Sun R. Kim, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, Korea 1 (2010).

408 Ibid. See also Hyun-Soo Kim, Trade secret law, intellectual property, and innovation: Theoretical, empirical, and Asian perspectives, PhD Thesis, University of Illinois (2011); Mirjana Stankovic, Trade Secrets: South Korea versus United States (2010): http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1678768.

409 AMCham Korea, Intellectual Property Rights (2004), http://www.amchamkorea.org/publications/2004ikbc/Intellectual%20Property%20Rights.doc.

410 2011 Investment Climate Statement – Republic of Korea, US Department of State (March 2011), http://www.state.gov/e/eb/rls/othr/ics/2011/157359.htm.

411 Office of the US Trade Representative, 2007 Special 301 Report 39 (2007).

> [T]rade secret' means technical or business information which is useful for any production and sale methods or other business activities which; (i) is not known to the public, (ii) has an independent economic value; and (iii) has been maintained in secret by considerable effort.[412]

As is the case in many countries, the information must indeed be secret; it must derive value from secrecy;[413] and the owner must take reasonable (also described as "substantial"[414] or, as above, "considerable") steps to safeguard secrecy. Under the case law, the sufficiency of the steps taken to guard secrecy is judged in accord with an "objective relevant industry standard."[415]

b. Scope and Subject Matter Under Civil Law

The scope and subject matter of trade secret protection in Korea is broad. Korean law protects both confidential business information and technical secrets as trade secrets.[416] Secrecy need not be absolute.[417] It must not be generally known to the public, but it may be disclosed to others provided that it is maintained as a secret. As discussed below, the law applies to both unrelated third parties (who may not misappropriate trade secrets) and parties with a contractual or other duty to the owner.

c. Scope and Subject Matter Under Criminal Law

The Trade Secret Act includes criminal sanctions for the same behavior and subject matter it sanctions under civil law.[418] Specifically, it imposes penalties for knowingly acquiring, using, or disclosing a trade secret for use in a foreign country, or for knowingly acquiring, using, or disclosing a trade secret for personal gain or to do damage to the owner.[419] In addition, other provisions of the Korean Criminal Code are used to prosecute trade secret theft, including for breach of fiduciary duty for misappropriating materials and files from one's workplace.[420]

3. Fault

a. Standard Under Civil Law

Korean trade secret law imposes liability on two different bases: (1) misappropriation; or (2) breach of duty.

---

412 Trade Secrets Act, Art. 1, Para. 2. Translation from: Sun R. Kim, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, Korea 2 (2010).

413 "The independent economic value requirement does not refer to the independent economic value of the trade secret itself," but rather to the competitive advantage conferred by secrecy. MacLaren, Trade Secrets Throughout the World § 24:5 (2012).

414 MacLaren, Trade Secrets Throughout the World § 24:4 (2012).

415 Ibid.

416 Sun R. Kim, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, Korea 2 (2010).

417 Ibid.; MacLaren, Trade Secrets Throughout the World § 24:15 (2012).

418 MacLaren, Trade Secrets Throughout the World § 24:15 (2012).

419 Trade Secrets Act, Art. 18; MacLaren, Trade Secrets Throughout the World § 24:6 (2012).

420 MacLaren, Trade Secrets Throughout the World § 24:6 (2012).

Article 2, Paragraph 1 of the Trade Secrets Act states that infringement means "Acquiring trade secrets by theft, deception, coercion or any other improper means ("acts of improper acquisition"), or subsequently using or disclosing the improperly acquired trade secrets (including informing any specific person of the trade secrets while under a duty to maintain secrecy."[421] Misappropriation thus includes various criminal acts and torts as well as a general category of improper means. "The term 'improper means' is interpreted to include all kinds of acts or means that violate social order founded upon sound trade and fair competition."[422]

Thus, misappropriation is understood broadly. It includes both acts that are wrongful per se, but also circumventing the owner's attempts to maintain secrecy. One authority provides a list demonstrating this breadth:

> Examples of misappropriation include, but are not limited to, the following: (1) in cases where the trade secret is preserved in a medium, such as booklets, tapes, etc., obtaining such medium through larceny, fraud, or coercion; (2) obtaining the trade secret through replication and photocopying of the medium in which the trade secret is preserved, contrary to the will of the holder of the trade secret; (3) acquiring knowledge or memorizing the trade secret after viewing the trade secret, contrary to the will of the holder of the trade secret; or (4) where the trade secret is not preserved in a medium but is kept, for example, in the memory of the owner, acquiring the trade secret by eavesdropping, wiretapping, or through physical assault, threat, or fraud.[423]

Under Korean law, trade secret infringement may also arise from breach of duty. Article 2, Paragraph 4 of the Trade Secrets Act states that infringement means "[u]sing or disclosing trade secrets to obtain improper benefits or to damage the owner of the trade secrets while under a contractual or other duty to maintain secrecy of the trade secrets."[424] Parties with a duty to maintain trade secrets include parties who are expressly bound by contract to do so, but may also include parties with an implied duty because of a fiduciary relationship.[425] As discussed below, such persons may include employees.

In addition, the Trade Secrets Act imposes liability beyond the initial wrongful act on both the original offender and on third parties. Article 2, Paragraphs 2, 3, 5, and 5 of the Trade Secrets Act impose liability for acquiring, using, or disclosing trade secrets with either knowledge, or gross negligence in not knowing, that they were acquired or disclosed by improper means or through breach of duty. Conversely, if a third party is innocent because it lacked knowledge or gross negligence, then he or she will not be liable.[426]

---

421 Trade Secrets Act, Art. 2, Para. 1. Translation from: Sun R. Kim, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, Korea 4 (2010).

422 Sun R. Kim, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, Korea 4 (2010).

423 MacLaren, Trade Secrets Throughout the World § 24:11 (2012).

424 Trade Secrets Act, Art. 2, Para. 4. Translation from: Sun R. Kim, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, Korea 4 (2010).

425 MacLaren, Trade Secrets Throughout the World § 24:15 (2012).

426 Sun R. Kim, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, Korea 4 (2010).

b. Standard Under Criminal Law

As discussed above, Article 18 of the Trade Secret Act imposes criminal penalties for certain intentional acts. Specifically, it sanctions knowingly acquiring, using, or disclosing a trade secret for use in a foreign country, or knowingly disclosing a trade secret for personal gain or to do damage to the owner.

4. Remedies

a. Remedies Under Civil Law

A wide array of remedies for trade secrecy infringement is available in Korea:[427]

- Preliminary and permanent injunctions and restraining orders.
- Compensatory damages, which include actual damages, plaintiff's lost profits, defendant's profits, or a reasonable royalty.
- Destruction of infringing goods.

b. Remedies Under Criminal Law

Article 18 of the Trade Secret Act imposes the following criminal penalties.

- A person who knowingly acquires, uses, or discloses a trade secret for use in a foreign country, "shall be subject to imprisonment not exceeding ten years, or to a fine not less than two times but not exceeding 10 times the proprietary profit amount."[428]
- A person who knowingly acquires, uses, or discloses a trade secret for personal gain or to do damage to the owner "shall be subject to imprisonment not exceeding five years, or to a fine not less than two times but not exceeding ten times the proprietary profit amount."[429]

5. Procedures

a. Emergency Action to Preserve Proof

There appears to be no provision under Korean law for an emergency action to preserve proof.

b. Pre-Trial Disclosure and Discovery

Korea does not have pre-trial discovery as such. Documentary evidence is taken at pre-trial hearings under the authority of the court.[430]

c. Secrecy During Litigation

Since 2012, trade secrets are protected during litigation. Pursuant to Article 163 of the Code of Civil Procedure "the court may limit by its ruling, upon the party's motion, the persons eligible to file a request for the perusal or copying of the portions containing any

427 Sun R. Kim, Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, Korea 5 (2010)

428 Trade Secrets Act, Art. 18. Translation from: MacLaren, Trade Secrets Throughout the World § 24:6 (2012).

429 Ibid.

430 International Civil Procedure § 5.2 (2003).

secrets from the litigation records, or for the delivery of an authentic copy, certified copy, or abridged copy of the portions containing any secrets from the litigation records".[431]

6. Employee-Employer Relationships

"[A]ccording to the prevailing view among legal scholars, a duty of confidentiality can be implied in most employment agreements."[432] In *Monami et al. v. Micro Ceramic*,[433] the Supreme Court held that the duty to keep trade secrets confidential under the Trade Secrets Act applies to those who have a duty of trust and good faith. Such persons would include any party with a fiduciary duty, and, most likely employees.[434] There is disagreement as to whether an implied duty continues after the end of employment.[435]

Express post-employment confidentiality obligations are enforceable if reasonable. However, "[t[he general knowledge, experience, and techniques obtained by the defendant during his employment [are] not included in the protected know-how or trade secrets."[436]

Post-employment covenants not to compete are also enforceable if they are reasonable, but they are viewed less favourably by courts than confidentiality agreements.[437] Such agreements must be reasonable due to the Constitutional right of freedom of employment. The factors considered include "the existence of protectable employer interests, a former employee's position in a former employer's firm, durational and geographical scope of the restraint, field of work, the existence of compensation offered to an employee, reasons for termination of the employment relationship, public interests, and so on."[438]

A court may enjoin a former employee from doing particular work for a competitor where trade secret appropriation is inevitable. On the one hand, a court may not enjoin an employee from working for a competitor at all based on the need to protect trade secrets. On the other, it may prohibit the employee, under exceptional circumstances, "from engaging in the trade secret-related work in the new firm as a necessary measure to prohibit or prevent the trade secret misappropriation on the basis of paragraph 1 of Article of 10 of the Trade Secret Act.[439]

7. Data Protection and Exclusivity

Pursuant to Article 18.9 of the Korea-US Free Trade Agreement, Korea now provides the following data exclusivity for regulatory test data:

- Five years of data exclusivity from the date of marketing approval for new pharmaceuticals.

---

431 MacLaren, Trade Secrets Throughout the World § 24:32 (2012).

432 MacLaren, Trade Secrets Throughout the World § 24:15 (2012).

433 Monami et al. v. Micro Ceramic, 96 Da 16605 (December 23, 1996).

434 MacLaren, Trade Secrets Throughout the World § 24:15 (2012).

435 Hyun-Soo Kim, Trade secret law, intellectual property, and innovation: Theoretical, empirical, and Asian perspectives, PhD Thesis, University of Illinois 139 (2011).

436 Ibid.

437 Ibid.

438 Ibid at 145 (translating and quoting Seoul Central District Court of Korea, Decision of Mar. 19, 2008, Case No. 2007kahap3903).

439 Ibid at 142 – 145 (translating and quoting Samsung Electronics Co. v. Pantech Co. Ltd., Supreme Court of Korea, Judgment of July 16, 2003, Case No. 2002ma4380).

- Three years of data exclusivity from the date of marketing approval for new clinical information for previously approved chemical entities.
- Ten years of data exclusivity for new agricultural chemical products.
- Ten years of data exclusivity for a new use of previously approved agricultural chemical products

Third parties cannot submit these data for the purpose of obtaining marketing approval for the same or a similar product, without the consent of the owner of the data.

8. Complementary Legal Institutions

On the Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, South Korea receives a score of 6.14 out of 10, which ranks it 55th in the world.[440] It ranks relatively low on judicial independence (4.59 out of 10) and impartial courts (3.71 out of 10).[441]

9. Technology Transfer

Korea does not subject foreign investors to technology transfer requirements.[442] Although technology licenses were regulated in the past, there are few remaining requirements. The Foreign Investment Protection Law restricts inbound licenses that interfere with national security or public order. It also requires that agreements be reported (but not approved) in the case of licenses that last more than one year and involve (i) aerospace; (ii) defence; or (iii) advanced technology.[443] This is a reporting, not approval, requirement.

440 Fraser Institute, Economic Freedom of the World 2011 Annual Report at 99 (2012).

441 Ibid.

442 Eckstrom's Licensing in Foreign and Domestic Operations: Joint Ventures § 17.4 (2013).

443 MacLaren, Trade Secrets Throughout the World § 24:25 (2012).

New Zealand

1. Overview

New Zealand is a common law country with a legal system and laws derived from and similar to the legal system and laws of England. New Zealand courts frequently look to the laws of the United Kingdom (and other common law nations) for guidance. Because of this legal heritage, New Zealand's trade secrecy law resembles UK trade secrecy law quite closely. New Zealand's courts frequently refer to and follow leading English decisions that are discussed in this paper's summary of UK law. At the same time, New Zealand's law of trade secrecy includes its own body of decisions. This summary will thus necessarily refer to UK law and will repeat portions of the UK summary, but will also take care to point out where New Zealand's law departs from or clarifies principles from UK law.

New Zealand protects trade secrets under both civil and criminal law. In fact, its only express, comprehensive statutory protection for trade secrets is a criminal statute, and thus the clearest definition of trade secrecy in New Zealand is in its criminal statute.

Trade secrecy law in New Zealand, at least the civil portion of it, is considered somewhat underdeveloped by some observers. One commentator described the situations as follows:

> By comparison with other larger common law jurisdictions, there has been limited case law on trade secrets and confidential information in New Zealand. Fact situations that have given rise to finer legal issues in other jurisdictions have not, as yet, been litigated in New Zealand. This means that some of the finer points of law have yet to be decided by a New Zealand court.[444]

Of course, as a common law country, New Zealand courts have resort to the decisions of other jurisdictions for guidance, particularly England, Australia, and Canada.

2. Scope and Subject Matter

All commercially valuable confidential information is potentially subject to trade secrecy protection. There does not appear to be a distinction between technical information (e.g., manufacturing diagrams or formulas) and non-technical business information (e.g., customer lists) under New Zealand's law.

a. Definitions

Definition Under Civil Law

New Zealand's law looks to a leading English case for the definition of trade secret. In *Coco v A.N. Clark (Engineers) Ltd.*,[445] Megarry, J., stated:

> In my judgment, three elements are normally required if, apart from contract, a case of breach of confidence is to succeed. First, the information must itself … 'have the necessary quality of confidence about it.' Secondly, that information must have been imparted in circumstances importing an obligation of confidence. Thirdly, there must be an unauthorised use of that information to the detriment of the party communicating it.

444 MacLaren, Trade Secrets Throughout the World § 29:1 (2012).

445 Coco v. A.N. Clark (Engineers) Ltd. [1969] RPC 41. Followed by courts in New Zealand, including AB Consol. Ltd. v. Europe Strength Food Co. Pty. Ltd., [1978] 2 NZLR 515.

In sum, a trade secret is information that:

1. Has a confidential quality, and the owner has attempted to limit dissemination;
2. Was disclosed to the defendant under confidential circumstances; and
3. Defendant has used or disclosed the information (or threatens to do so) to the detriment of the owner.

Definition Under Criminal Law

In 2003, New Zealand added a criminal statute addressing trade secrets. Section 230(2) of the Crimes Act 1961 defines trade secret as follows:

(2) For the purposes of this section, trade secret means any information that—

(a) is, or has the potential to be, used industrially or commercially; and

(b) is not generally available in industrial or commercial use; and

(c) has economic value or potential economic value to the possessor of the information; and

(d) is the subject of all reasonable efforts to preserve its secrecy.

Two authorities note that there appears to be no case law concerning Section 230.[446]

b. Scope and Subject Matter Under Civil Law

General Subject Matter. New Zealand courts interpret the subject matter of trade secret law broadly, covering both confidential business information and technical information. An action may "be brought in relation to manufacturing and product technology, confidential business information, including lists of customers (both current and prospective), and lists of suppliers."[447] Notably, the New Zealand's courts have rejected[448] the distinction made in the English case of *Faccenda Chicken Ltd. v. Fowler*,[449] between business information and "secret processes of manufacture." A leading treatise[450] compiled the following list of examples from New Zealand's case law, which demonstrates the breadth of business information covered by New Zealand's law:

- economic forecasts provided to subscribers
- a defrosting technique that required low temperatures to be successful
- a manufacturing process, each step of which was well known in the industry, but the overall process was not
- malt extract manufacturing processes
- the workings of a machine of which there were only three in New Zealand

446 MacLaren, Trade Secrets Throughout the Word § 29:4 (2012); Paul Sumpter, Intellectual Property Law: Principles in Practice 326 (2006).

447 MacLaren, Trade Secrets Throughout the Word § 29:3 (2012) (citing cases).

448 SSC&B: Lintas New Zealand Ltd. v. Murphy & Anor, (1986) 3 NZCLC 99,546.

449 [1986] 1 All ER 617

450 The list is quoted in its entirety from MacLaren, Trade Secrets Throughout the World § 29:7 (2012) (citations to cases omitted).

- business forms
- a process for making scented paper
- a formula for a mould release agent
- confidential plans covering commercial projects.

Confidential Quality. The information that is the subject of trade secrecy must not be in the public domain. Secrecy need not be absolute, but dissemination must be limited to parties with some obligation to keep the information secret.[451] Once information enters the public domain, at least through the fault of plaintiff, it generally ceases to be confidential.[452] Courts will consider the extent of the measures taken by plaintiff to secure the information, as well as how widely it is known within and outside of the business.[453]

Disclosed to the Defendant Under Confidential Circumstances. New Zealand's courts cite the requirement from *Coco v. A.N. Clark*[454] and other English cases that the information must be communicated under conditions that create an obligation of confidentiality. As discussed in this paper's summaries of UK law, this requirement may suppose that there must be some relationship between the parties. However, as also discussed in summaries of UK and Australian law, those jurisdictions appear to have evolved away from this requirement. However, this is not the case with New Zealand's law.

As one commentator puts it, the "New Zealand approach is likely to be more traditional, at least as hinted by the Court of Appeal in the ground-breaking privacy case *Hosking v Runting.*"[455] Two of the judges in that case expressed concern that the law of trade secrets "should not be strained beyond its traditional boundaries."[456] The commentator concludes that it appears that New Zealand continues to require that there "be a relationship importing confidentiality obligations."[457]

Thus New Zealand appears to maintain the relationship-based view of trade secret infringement. Courts will thus look to a breach of duty, rather than misappropriation (or breach of a broadly implied duty) via surveillance or trespass. Nevertheless, courts also will likely impose a duty on a third party that receives information as a result of breach of duty by another, at least if the third party does so knowingly.[458]

---

451 Coco v. A.N. Clark Eng'rs Ltd., [1969] RPC 41; AB Consol. Ltd. v. Europe Strength Food Co. Pty. Ltd., [1978] 2 NZLR 515.

452 MacLaren, Trade Secrets Throughout the World § 29:7 (2012) (citing Ceiling Care (NZ) Ltd. v. Smith, unreported, Auckland A1337/83, 9 Oct. 1987, Wylie, J.; Sanitation Servs. (NZ) Ltd. v. Dahlin, unreported, Auckland A203/79, 21 May 1980, Speight, J.; Bendon Indus. Ltd. v. Presslok Indus. Ltd., (1982) 1 TCLR 61.).

453 AB Consol. Ltd. v. Europe Strength Food Co. Pty. Ltd., [1978] 2 NZLR 515.

454 Coco v. A.N. Clark Eng'rs Ltd., [1969] RPC 41; AB Consol. Ltd. v. Europe Strength Food Co. Pty. Ltd., [1978] 2 NZLR 515.

455 Paul Sumpter, Intellectual Property Law: Principles in Practice 306 (2006) (citing Hosking v. Runting [2005] 1 NZLR 1 (CA)).

456 Ibid.

457 Ibid.

458 Ibid. at 310 - 311.

Use or disclosure of information to the detriment of the owner. In the recent case of *Fisher & Paykel Finance v Karum*, the New Zealand high court held that a defendant had not infringed trade secrets because, in part, the confidential information viewed was not substantial enough to harm the plaintiff.[459] In most instances such harm is likely to be present,[460] but the requirement might prove problematic for a party that owns but does not use or intend to use information. (For example, this may be the case with information about the second-best way to manufacture a product, where the owner is already using the best method.)

c. Scope and Subject Matter Under Criminal Law

Section 230(1) of the Crimes Act 1961 defines an offense of taking, copying, or obtaining trade secrets as follows:

> (1) Everyone is liable to imprisonment for a term not exceeding 5 years who, with intent to obtain any pecuniary advantage or to cause loss to any other person,—
>
> (a) dishonestly and without claim of right, takes, obtains, or copies any document or any model or other depiction of any thing or process containing or embodying any trade secret, knowing that it contains or embodies a trade secret; or
>
> (b) dishonestly and without claim of right, takes or obtains any copy of any document or any model or other depiction of any thing or process containing or embodying any trade secret, knowing that it contains or embodies a trade secret.

What is notable is that this offense appears to cover only taking, obtaining or copying the physical embodiment of the trade secret. This criminal provision thus does not represent much of a difference from essentially every other country where theft of documents or other physical media constitutes an offense. However, it does accomplish two things that the general prohibition on theft might not. First, in other countries, returning a document after obtaining or copying the information from it might avoid a theft charge (for example, this is the case in the United Kingdom). This provision appears to cover such an action. Second, the severity of punishment for theft is often tied to the value of what was stolen. In a country that relies on a general prohibition against theft, the value of a stolen document or data storage device might be determined by the trivial value of the thing itself and not the information it contains. This provision creates a serious offense based on the value of the information on the medium.

3. Fault

a. Standard Under Civil Law

Civil trade secrecy law in New Zealand does not frame the cause of action for trade secret in terms of fault, such as through intentional or negligent disclosure. Rather, as discussed earlier, the offense is in using or disclosing the information in breach of a duty not to do so, regardless of whether the using or disclosing party intends to breach the duty or harm the claimant. This is particularly the case since New Zealand apparently maintains the relationship-based view of trade secrecy protection.

---

459 Fisher & Paykel Finance v Karum, [2012] NZHC 3314. The court stated that “having regard to the scale, duration and complexity of the project" the instances where software source code were reviewed were limited in number and “none involved a deliberate attempt to appropriate protected information and none resulted in detriment to Karum”.

460 Paul Sumpter, Intellectual Property Law: Principles in Practice 307 - 308 (2006). See also Coco v. A.N. Clark Eng'rs Ltd., [1969] RPC 41.

In the case of a third party who obtains information as a result of a breach of another's duty, it appears that the third party must have knowledge of the breach.[461] One commentator opines that truly innocent third parties may be excused from liability: "Clearly, there will be degrees of knowledge, ranging from actual knowledge to situations where a reasonable person, knowing of the circumstances, would or should raise the question as to whether or not the information was confidential. . . . [I]t seems that it would usually be necessary that a third party have some degree of knowledge, but it is unclear precisely at what point someone can be said to have enough knowledge to be fixed with the obligation."[462] However, there is case law where a third party that hires an employee of a competitor is imputed with knowledge if the new employee proceeds to use a trade secret in breach of duty.[463]

b. Criminal Law

Under Section 230(1) of the Crimes Act 1961, culpability is based on the "intent to obtain any pecuniary advantage or to cause loss to any other person."

4. Remedies

a. Civil Law

The following remedies are available:

- Injunctive relief, both interlocutory and permanent.[464]
- Seizure and destruction of infringing materials pursuant to an order for delivery up.[465]
- Monetary relief, either in the form of compensatory damages or recovery of defendant's profits.[466] Exemplary damages are not available.[467]

Injunctive relief is not mandatory. If a defendant's actions effectively make the information public, then the information may no longer be confidential, thus precluding an injunction,[468] but not monetary remedies. Even where information has become public, a defendant may be enjoined for a limited period to negate its improper "head start" in obtaining the information under the "springboard" doctrine.[469]

b. Criminal Law

Under Section 230(1) of the Crimes Act 1961, the penalty is up to 5 years of imprisonment.

461 Hunt v. A, [2008] 1 NZLR 368.

462 Paul Sumpter, Intellectual Property Law: Principles in Practice 311 (2006) (footnotes omitted).

463 Ibid. (citing Cranleigh Precision Engineering, Ltd v. Bryant [1966] RPC 81).

464 MacLaren, Trade Secrets Throughout the Word, § 29.12 (2012).

465 MacLaren, Trade Secrets Throughout the Word, § 29.12 (2012)

466 MacLaren, Trade Secrets Throughout the Word, § 29.13 (2012).

467 MacLaren, Trade Secrets Throughout the Word, § 29.13 (2012).

468 Aquaculture Corp. v. New Zealand Green Mussel Co. Ltd. (No. 1), (1985) 5 IPR 353.

469 Ibid.

5. Procedures

a. Emergency Action to Preserve Proof

In New Zealand, as in the United Kingdom, an ex parte procedure known as an Anton Piller Order is potentially available to plaintiffs seeking to preserve proof.[470] The procedure allows the plaintiff to apply directly to the court without informing the potential defendant. If granted, the plaintiff may search the defendant's premises and seize documents. The order allowing this procedure may be no more broad than is necessary to preserve the relevant evidence. An Anton Piller Order is granted at the discretion of the court upon a showing that it is necessary to preserve evidence. As discussed in this paper's summary of UK law, Anton Piller orders have proven to be controversial in some cases. This remedy is thus limited to cases "where there is strong evidence, higher than that needed for an interim injunction, for example; and that irreparable harm will or may occur to the plaintiff unless the remedy is granted."[471]

b. Pre-Trial Discovery

In New Zealand, pre-trial discovery is available but generally limited to documentary evidence.

c. Secrecy During Litigation

In New Zealand, a wide array of procedures to safeguard the secrecy of plaintiff's confidential information is available during trade secret litigation. The plaintiff can obtain closed or "in camera" hearings for both pre-trial procedures and the trial.[472] They also may obtain protection from the opposing party, limiting access to particular information or access to counsel or certain experts or professionals on the case.[473]

6. Employee-Employer Relationships

New Zealand's law enforces both implied and express duties imposed on employees to keep information confidential, but is also protective of employee's ability to earn a living after leaving an employer.[474] New Zealand's courts will enforce express contractual duties to keep information confidential, both during and after employment, but may limit them after employment.

Like UK law, New Zealand's law distinguishes between the duties of current and former employees with respect to the *types* of confidential information protectable. While employed, an employee has a broad implied duty of fidelity that covers confidential and sensitive information generally.[475] This broad duty ceases at the end of employment. However, an employee has a narrower implied duty of confidentiality with respect to information that is developed specifically by the employer that otherwise meets the definition of trade secrecy.[476] As in the United Kingdom, it appears that the distinction lies between the employee's

470 Busby v. Thorn EMI Video Programmes Ltd. [19840 NZLR 461 (CA) (recognizing Anton Piller orders in New Zealand).

471 Paul Sumpter, Intellectual Property Law: Principles in Practice 325 (2006).

472 MacLaren, Trade Secrets Throughout the Word, § 29.18 (2012).

473 MacLaren, Trade Secrets Throughout the Word, § 29.18 (2012).

474 Ibid § 29.8.

475 Ibid § 29.10.

476 Ibid.

unprotected general skills and knowledge that will enable them to earn a living, and detailed business information and technical secrets specific to the employer.[477]

Express agreements to keep information confidential after employment, may be broader than a post-employment implied duty, and are more likely to be enforced. However, they are not certainly enforceable. Agreements that purport to restrain an employee from exercising general skills and knowledge are likely unenforceable.[478]

New Zealand's courts, however, are reluctant to enforce either trade secret agreements or covenants not to compete if they affect an employee's ability to earn a living.[479] A guiding consideration is to allow former employees to exercise skills and general knowledge so as not to impede employment prospects. Moreover, duties will not be enforced unless there is a competitive need to do so and the limitations are reasonable with respect to time and geographic scope.[480]

7. Data Exclusivity and Data Protection

New Zealand provides 5 years of data exclusivity for drugs with new active components and new agricultural chemicals.[481] During the period of exclusivity, which begins on the date of registration, no other party may receive the registrant's data nor may they rely on it for an application to register an equivalent product. There is no data exclusivity period for data relating to new uses or formulations of old active ingredients.

8. Complementary Legal Institutions

New Zealand is very highly regarded for its commercial legal system. It is among the most reliable and effective for contract and property rights enforcement. On the Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, New Zealand receives a score of 9.03 out of 10, which ranks it 6th in the world.[482]

9. Technology Transfer

New Zealand does not subject foreign investors to technology transfer requirements, joint venture technology contribution requirements, or license registration requirements.[483]

---

477 Ibid (citing cases).

478 Paul Sumpter, Intellectual Property Law: Principles in Practice 319 - 320 (2006).

479 MacLaren, Trade Secrets Throughout the Word, § 29.8 (2012); Paul Sumpter, Intellectual Property Law: Principles in Practice 318 - 320 (2006).

480 MacLaren, Trade Secrets Throughout the Word, § 29.8 (2012); Paul Sumpter, Intellectual Property Law: Principles in Practice 318 - 320 (2006).

481 In correspondence with the OECD Secretariat (October 2013), the New Zealand authorities noted that the Government recently announced that a further three years of protection will be provided in cases of new uses of known compounds.

482 Fraser Institute, Economic Freedom of the World 2012 Annual Report at 124 (2012).

483 MacLaren, Trade Secrets Throughout the Word, § 29.14 – 29.15 (2012).

Russian Federation

1. Overview

In Russia, the law of trade secrets is relatively new and still under development. There are certain requirements under the Commercial Secrets Law for obtaining trade secret protection – essentially formalities – that limit the utility of Russian trade secret law. In addition, various governments, commentators, and surveys of business people have indicated serious concerns about trade secret theft within, and initiated from, Russia.

Protection of trade secrets is a very recent development in Russian law. Trade secrets did not appear in Russian law until after the end of the Soviet era. In the 1990s, disclosure of commercial or trade secrets was specified as a form of unfair competition under laws addressing enterprises and competition.[484] After several years of uncertainty, a definition of trade secret was supplied in Article 139 of the Civil Code.[485] However, it was not until 2004 that the Commercial Secrets Law[486] was passed, and some commentators consider this law to be the first trade secret law in Russia.[487] In 2006, the law was significantly clarified and strengthened, with remedies added, as part of a comprehensive reform of intellectual property laws that consolidated intellectual property laws into a new Fourth Part of the Civil Code. The laws became effective on 1 January 2008. Russian trade secret law is thus relatively new and not yet fully developed in some respects.

A number of concerns have been expressed about enforcement of trade secret law in Russia. In February 2013, the Executive Office of the President of the United States released a report on trade secret theft entitled "Administration Strategy on Mitigating the Theft of US Trade Secrets."[488] In addition to setting forth a strategy, the report gathered several previous US government assessments of the trade secret problem, including a 2011 report by the Office of the National Counterintelligence Executive.[489] This report identifies Russia as posing a "pervasive threat" as one of the two most "aggressive collectors" (the other one identified was China) "of US economic information and technology."[490] In the days and weeks that followed release of the Administration Strategy, senior US officials frequently promoted the strategy and cited Russia along with China as threats. Other governments have similarly singled out

484 Terrence F. MacLaren, Evgeny Alexandrov and Natalia Stepanova, 3 Trade Secrets Throughout the World § 32:2 (2012) (hereafter "MacLaren, Trade Secrets Throughout the World").

485 MacLaren, Trade Secrets Throughout the World § 32:2 (2012).

486 Federal'nii Zakon "O Kommercheskoy Tayne" [Federal Law on Commercial Secrecy] No. 98-FZ, July 27, 2004, 32 SZ RF item 3283 (2004), amended by Federal Law No. 19-FZ, Feb. 2, 2006, 6 SZ FR item 636 (2006) ("Commercial Secrets Law").

487 See Sergey Budylin & Yulia Osipova, Total Upgrade: Intellectual Property Law Reform in Russia, 1 Colum. J.E. Eur. L. 1, 5 (2007) (describing first intellectual property protection for trade secrets as dating from 2004 in Commercial Secrets Law). See also MacLaren, Trade Secrets Throughout the World § 32:2 (2012), which states: "Obviously, existence of a single Article in the Law could not meet the requirements of the quickly developing business which needed detailed and clear regulation of relations regarding spreading of information having commercial value."

488 Executive Office of the President of the United States, Administration Strategy on Mitigating the Theft of US Trade Secrets (February 2013).

489 Office of the National Counterintelligence Executive Report, Foreign Spies Stealing US Economic Secrets in Cyberspace (2011).

490 Ibid at 4 - 5.

Russia as a source of trade secret theft.[491] For example, the head of Germany's military intelligence stated that one of his agency's main priorities was combatting industrial espionage from China and Russia.[492]

Comments from the business sector have echoed these poor perceptions regarding Russia's actions with respect to trade secrets. In 2009, the security firm McAfee surveyed "1 000 senior IT decision makers in the US, UK, Japan, China, India, Brazil and the Middle East."[493] The report found that nearly 50% of respondents rated the "threat level" to their sensitive data in Russia as "high."[494] The report related the following perceptions:

> Three countries, in particular, stood out to the survey respondents—perhaps reflecting broader security perceptions. Respondents cited China, Pakistan and Russia as the worst-rated countries when it comes to the protection of digital assets. Pakistan, China and Russia, in that order, were also perceived to have the worst reputations for pursuing or investigating security incidents. Respondents cited corruption among law enforcement and the legal systems as well as poor skills among law enforcement as top reasons for the reputation rating.[495]

The report also found that nearly 20% of respondents had avoided doing business in Russia due to security concerns.[496] A 2011 survey of international business executives by McAfee and SAIC found these concerns about Russia unabated, as survey respondents once again ranked Russia among the top three security threats and among the top three countries where they avoided doing business due to security threats.[497]

Russian experts echo these concerns. As one Russian lawyer advised in an article about contributing know-how into Russia for purposes of foreign direct investment, "even a carefully drafted agreement does not guarantee confidentiality in trade secret utilization by the licensee's employees. Often, foreign investors dealing in Russia face [a] low standard of ethics and responsibility adhered [to] by Russian contractors and employees. Russian labor law is not flexible enough to ensure [the] effective protection which foreign investors may expect."[498]

2. Scope and Subject Matter

a. Definitions

Russian law defines trade secrets in terms similar to the law of most countries, with one notable and significant limitation. It does not distinguish between technical secrets and confidential business information. In fact, it uses several terms interchangeably when referring

491 Ibid at Appendix B-1.

492 Reuters, German Spy Chief Targets Russian, Chinese Industrial Espionage, 18 February 2013, http://www.reuters.com/article/2013/02/18/us-germany-spies-idUSBRE91H08C20130218.

493 McAfee, Unsecured Economies: Protecting Vital Information 1, 2 (2009).

494 McAfee, Unsecured Economies: Protecting Vital Information 1, 12 (2009).

495 McAfee, Unsecured Economies: Protecting Vital Information 1, 13 (2009).

496 McAfee, Unsecured Economies: Protecting Vital Information 1, 14 (2009).

497 McAfee, Underground Economies: Intellectual Capital And Sensitive Corporate Data Now The Latest Cybercrime Currency 10 (2011).

498 Artem Sirota, On contributing know-how in capital of Russian company, http://www.russianlawonline.com/content/contributing-know-how-capital-russian-company.

to trade secrets, which are translated as commercial secrecy, secrets of production and know-how, a group of terms that several commentators say can be referred to under the general term "trade secrets."[499]

Article 1465 of the Civil Code defines trade secrets as confidential information as follows: [500]

- "[Information of] any type (production, technological, economic, organizational and others), including information on the results of intellectual activity in the area of science and technology and information on methods of carrying out the professional activity;"
- that has "real or potential commercial value because it is unknown to third persons;"
- to which third parties do not have legally permissible open access; cannot be accessed freely by third parties legally;
- and that is subject to a regime of commercial secrecy (which is defined in Article 10 of the Commercial Secrecy Law).

Thus, under Russian law, just like the law of many countries, a trade secret is confidential technical or commercial information that derives value from secrecy and is actually secret. The information remains protectable as a trade secret for so long as it remains confidential. Once the information is disclosed, trade secret protection ends for all holders of the trade secret (including those who have developed it independently).[501]

Like most countries, Russia requires the owner of the trade secret to make efforts to maintain secrecy, but, less commonly, it prescribes mandatory steps for maintaining secrecy. These mandatory measures limit the scope of trade secret protection in Russia.

b. Scope and Subject Matter Under Civil Law

The scope of trade secret protection in Russia is potentially broad based on how trade secrets are defined, but it is, in practical terms, severely limited by additional requirements set by the Commercial Secrets Law. Article 10 of the Commercial Secrets Law sets forth the "regime of secrecy" that defines a trade secret pursuant to Article 1465 of the Civil Code. It lists the following measures that the owner of a trade secret must take to protect confidential information:[502]

- Create an inventory of trade secrets that defining the information to be treated as a trade secret;
- Limit access to the protected information;
- Keep a record of all persons allowed to access the protected information and/or to whom the protected information has been disclosed;

499 MacLaren, Trade Secrets Throughout the World § 32:3 (2012); Heidi Paalanen-Koev, Corporate Counsel's Guide to Doing Businsess in Russia § 4:47 (2012); Sergey Budylin & Yulia Osipova, Total Upgrade: Intellectual Property Law Reform in Russia, 1 Colum. J.E. Eur. L. 1, (2007).

500 Civil Code Art. 1465 (2011), ROSPATENT Unofficial English Translation, available at: http://www.rupto.ru/rupto/nfile/3b05468f-4b25-11e1-36f8-9c8e9921fb2c/Civil_Code.pdf.

501 Civil Code Art. 1467 (2011), ROSPATENT Unofficial English Translation, available at: http://www.rupto.ru/rupto/nfile/3b05468f-4b25-11e1-36f8-9c8e9921fb2c/Civil_Code.pdf.

502 Federal Law Commercial Secrecy, No. 98-FZ, Article 10 (July 29, 2004) (as amended 24 July 2007).

- Include a confidentiality clause in employment contracts and agreements with third parties that ensures these requirements are met; and
- Affix a "Commercial Secret" notice to documents containing trade secrets. This notice must list the full name and address of the owner.

Failure to comply with this regime, or to ensure that one's employees and business partners comply with it, disqualifies information from trade secret protection. As one commentator observes, "If an entity omits to follow any of the steps to establish a trade secrets regime, it may be unable to protect its trade secrets under the law. Among other things, this will prevent it from:

- bringing a criminal or administrative prosecution for violation of its trade secrets regime;
- claiming damages; and
- terminating an employee for disclosure."[503]

These requirements have several effects that narrow the scope of trade secret protection:

- They preclude implied duties to protect trade secrets. All employees and business partners must sign agreements.
- The inventory requirement effectively constitutes a requirement that the trade secret be both reducible to writing and actually reduced to writing. The requirement for an inventory is an added formality.
- The record-keeping requirement of access is, in practice, rather demanding, and constitutes yet another formality.
- The secrecy notice requirement for documents constitutes yet another formality. As a result of this requirement, the secrecy of a document may not be inferred from the circumstances. It appears to apply even within the context of a confidential relationship, so, for example, intra-office communications would need to be marked. Moreover, the requirement goes beyond even the practice of stamping a document "confidential," to require the inclusion of an address.

Experts have observed that these provisions have the effect of narrowing the scope of trade secret law in Russia by imposing impractical requirements. As one commentator observed, due to the regime of secrecy requirement, what would otherwise be "broadly interpreted [as] confidential information may fall outside the law's scope of protection."[504] Another commentator critiqued the law as follows: "The procedures are quite formal and inflexible, and the law can be criticized as already having been out-dated when it first came into force.

503 Denis I. Khabarov, Intellectual Property – Russia, International Law Office (January 2012) http://www.internationallawoffice.com/newsletters/detail.aspx?g=607f61de-b2f5-4f8f-a815-aa83e0e161e1.

504 Denis I. Khabarov, Intellectual Property – Russia, International Law Office (January 2012) http://www.internationallawoffice.com/newsletters/detail.aspx?g=607f61de-b2f5-4f8f-a815-aa83e0e161e1.

The procedures set forth by the law do not necessarily reflect the reality or the needs of a modern information society."[505]

c. Scope and Subject Matter Under Criminal Law

Article 183 of the Russian Criminal Code makes it an offense to gather, disclose, or receive commercial or trade secrets without the permission of the owner. The Criminal Code does not contain a unique definition of the term commercial or trade secret. Thus, the definition, scope, and subject matter of trade secret appear to be the same between civil and criminal law.

3. Fault

a. Standard Under Civil Law

Russian law essentially treats trade secret rights as property rights, with the owner having an exclusive right to use the information pursuant to Articles 1466 and 1229 of the Civil Code.[506] The law, however, allows for independent discovery and consequently, parallel ownership of a trade secret, "who has received the information constituting the content of the protected secret of production in good faith and independently from other holders of the secret of production."[507]

The consequence of treating trade secrets as property is that the standard for what is typically called misappropriation is, in theory, broader than in most other countries. By contrast and for example, in the US and the UK, trade secret liability is based on misappropriation, a concept that considers the circumstances under which the information was obtained. Russia treats the rights of a trade secret owner as exclusive rights, just as it does with respect to patents and copyrights. Indeed, it provides for trade secret remedies, including injunctions and damages, in Article 1252, the same general section of the Civil Code that designates remedies for all exclusive rights such as patents and copyrights.

The breadth of this protection is narrowed, somewhat, by the fact that Article 1472(2) contains a defence for parties that obtain trade secrets without knowledge of illegality. Article 1472(2) excuses from liability a "person who has used a secret of production and [was] not aware and shall not have a reason to [be] aware that the using is illegal, including with regard to the fact that he has obtained access to the secret of production accidentally or by mistake."[508] As a result, a party who obtains a trade secret is liable for damages only "if he did not know or should not have known that his use was unlawful, including in connection with

505 Heidi Paalanen-Koev, Corporate Counsel's Guide to Doing Business in Russia § 4:4 (2012).

506 Article 1466. Exclusive Right to a Secret of Production

1. The exclusive right to use a secret of production in accordance with Article 1229 of the present Code in any manner unrepugnant to a law (the exclusive right to a secret of production), including manufacturing and implementation of economic and organizational solutions shall belong to the owner of the secret of production.

Civil Code Art. 1466(1) (2011), ROSPATENT Unofficial English Translation, available at: http://www.rupto.ru/rupto/nfile/3b05468f-4b25-11e1-36f8-9c8e9921fb2c/Civil_Code.pdf.

507 Civil Code Art. 1466(2) (2011), ROSPATENT Unofficial English Translation, available at: http://www.rupto.ru/rupto/nfile/3b05468f-4b25-11e1-36f8-9c8e9921fb2c/Civil_Code.pdf.

508 Civil Code Art. 1472(2)(2) (2011), ROSPATENT Unofficial English Translation, available at http://www.rupto.ru/rupto/nfile/3b05468f-4b25-11e1-36f8-9c8e9921fb2c/Civil_Code.pdf

the fact that he obtained access to the know-how accidentally or by mistake."[509] However, in the part of the Civil Code addressing remedies for intellectual rights generally, a category which includes exclusive rights such as trade secrets, Article 1250 states that "[t]he absence of fault of an infringer shall not excuse him from the obligation to cease infringement . . . ." Thus, it appears that while a trade secret defendant who receives trade secrets without knowledge is excused from payment of damages, they still are subject to injunctive relief (but see the discussion below with respect to injunctive relief).

Notwithstanding this limitation on damages for "innocent" infringement, it appears that liability is potentially broader under Russian law for trade secret misappropriation than in many other countries. By contrast, in other countries, even when a party knowingly acquires a trade secret, that party will not be liable unless the acquisition of it constitutes misappropriation. Thus, in the United States, for example, a plaintiff must show that the defendant has acquired the confidential information by improper means, i.e., by using means that violate commercial morality or that would require plaintiff to incur excessive costs to prevent. By contrast, it appears that in Russia it may be the case that the plaintiff need only show that defendant acquired the information in violation of plaintiff's exclusive rights, regardless of the means used. However, the Russian law is still relatively new, and adjudication and expert opinion on this issue does not appear to exist at this point.

b. Standard Under Criminal Law

Russian criminal law imposes liability for intentional trade secret theft. It makes a distinction between acquisition on the one hand, and disclosure and use on the other. Under Article 183(1) of the Russian Criminal Code,[510] intentionally gathering trade secrets by theft of documents, bribery, threats, or other illegal means is punishable by fines or imprisonment. Under Article 183(2), the intentional unauthorized use or disclosure of trade secrets by an employee or other person entrusted with them is also punishable by slightly larger fines or longer prison sentences.

4. Remedies

a. Remedies Under Civil Law

Russian law provides remedies including compensatory damages, confiscation of the infringing goods, and, in theory, injunctions. Since trade secrets are an exclusive right (a category that includes patents and copyrights), a trade secret owner should be able to obtain the rights applicable to all exclusive rights under Article 1252(1) of the Civil Code. These remedies include (1) declaratory judgments; (2) injunctions; (3) damages; (4) seizure of infringing goods; and (5) publication of the judgment of infringement.[511] Preliminary seizure of infringing goods is also available pursuant to Article 1252(2) of the Civil Code.512 Damage awards for trade secret infringement are also specified in Article 1472(1) of the Civil Code. Under Article 15 of the Civil Code, when the remedy of damages is specified (as it is in

509 MacLaren, 3 Trade Secrets Throughout the World § 32:7 (2012).

510 Article 183(1), Criminal Code of the Russian Federation No. 63-FZ of June 13, 1996 (as last amended on June 29, 2009).

511 Civil Code Art. 1252(1) (2011), ROSPATENT Unofficial English Translation, available at: http://www.rupto.ru/rupto/nfile/3b05468f-4b25-11e1-36f8-9c8e9921fb2c/Civil_Code.pdf.

512 Civil Code Art. 1252(2) (2011), ROSPATENT Unofficial English Translation, available at: http://www.rupto.ru/rupto/nfile/3b05468f-4b25-11e1-36f8-9c8e9921fb2c/Civil_Code.pdf.

Articles 1252(1) and 1472(1)), it includes general compensatory damages, special compensatory damages, lost profits, punitive damages, and defendant's profits, but not consequential damages.513

Expert opinion casts doubt on whether injunctive relief is practicable in trade secret cases, at least with respect to former employees. Under Russian Law, a trade secret is an exclusive right "in accordance with Article 1229 of the Civil Code."[514] Article 1252 sets forth remedies for exclusive rights, which include "preventing the actions infringing the right or creating a threat of tis infringement."[515] It thus appears that injunctive relief for trade secret infringement is available under Russian law.

However, expert opinion casts doubt on the practical availability of injunctive relief in trade secret cases. In the case of *OJSC TNK-BP Holding v. Lazurenko*,[516] the English courts found it necessary to apply Russian trade secret law. Expert opinion on Russian law caused the High Court of London to dissolve an injunction granted by the lower court. The expert stated: "[I]t is theoretically possible to seek judicial prohibition to the defendant to undertake particular actions in relation to protected information as an injunctive relief measure under Article 140 of the RF Civil Procedure Code . . . but we are unaware whether the Russian courts have ever granted any such injunction to secure the employer's claim seeking compensation of damages caused by unauthorized disclosure by the employee of the protected information."[517] The London High Court thus concluded: "Accordingly, it is clearly Mr. Rozenberg's view that under Russian law commercially confidential information may not be protected by a *quia timet* injunction, whether interim or final." This conclusion appears to contradict Article 1252, which provides for a remedy "preventing the actions infringing the right or creating a threat of this infringement," but also may reflect actual experience.[518]

b. Remedies Under Criminal Law

The Russian Criminal Code sets forth three levels of penalties for trade secret theft:[519]

- First, "gathering of commercial information classified as a commercial . . . secret, by means of stealing documents, bribery and threats as well as in other illegal ways"[520] is

513 Christopher Osakwe, Russian Civil Code. Parts 1 -3: Text and Analysis 251 – 252 (2008).

514 Civil Code Art. 1466 (2011), ROSPATENT Unofficial English Translation, available at: http://www.rupto.ru/rupto/nfile/3b05468f-4b25-11e1-36f8-9c8e9921fb2c/Civil_Code.pdf.

515 Civil Code Art. 1252 (2011), ROSPATENT Unofficial English Translation, available at: http://www.rupto.ru/rupto/nfile/3b05468f-4b25-11e1-36f8-9c8e9921fb2c/Civil_Code.pdf.

516 [2012] EWHC 2781 (Ch).

517 [2012] EWHC 2781 (Ch).

518 See also, Artem Sirota, Major problems of contribution of the rights to the knowhow (trade secret) as an investment in the charter (share) capital of a Russian company, http://www.sirotamosgo.ru/publications/mpc/, April 2011, stating "The remedies for trade secret infringement are limited to direct, real damages incurred as the result of the trade secret infringement. Lost profit cannot be recovered."

519 Article 183, Criminal Code of the Russian Federation No. 63-FZ of June 13, 1996 (as last amended on 29 June 2009), translation available at http://www.wipo.int/wipolex/en/text.jsp?file_id=202465.

520 Article 183, Criminal Code of the Russian Federation No. 63-FZ of June 13, 1996 (as last amended on 29 June 2009), translation available at http://www.wipo.int/wipolex/en/text.jsp?file_id=202465.

"punishable with a fine of up to 80 thousand rubles, or six to twelve months' wage, or up to two years imprisonment."[521]

- Second, the intentional unauthorized use or disclosure of trade secrets by an employee or other person entrusted with them is "punishable with a fine of up to 120 thousand rubles or up to twelve months' income" or with "a deprivation of the person of his/her right to occupy certain offices or engage in certain activities for a term of up to three years;" or up to three years imprisonment.[522]
- Third, where the actions cause large-scale harm (damages exceeding 250 000 rubles) or are committed with a selfish or mercenary motive, punishment is elevated to a fine of up to 200 000 rubles or 18 months income with "a deprivation of the person of his/her right to occupy certain offices or engage in certain activities for a term of up to five years;" or up to five years imprisonment.[523]

5. Procedures

a. Emergency Action to Preserve Proof

Under Article 64 of the Civil Procedure Code of the Russian Federation, a party that fears for the security of evidence may apply to the court to secure this proof either before or after an action has commenced. [524] These motions are most commonly filed in intellectual property cases to preserve proof of infringement.[525] Actions taken may include a search with the participation of the court bailiff and seizure of evidence.[526]

b. Pre-Trial Disclosure and Discovery

Limited pre-trial discovery and disclosure is available under Russian Civil Procedure. However, uses of even the limited pre-trial discovery processes "are few and far between."[527] In the Russian judicial system, such processes take place under the supervision of the judge rather than between the parties.[528] Most discovery occurs at trial. Moreover, there is no requirement to engage in full disclosure prior to the commencement of trial. As a

521 Article 183, Criminal Code of the Russian Federation No. 63-FZ of June 13, 1996 (as last amended on 29 June 2009), translation available at http://www.wipo.int/wipolex/en/text.jsp?file_id=202465.

522 Article 183, Criminal Code of the Russian Federation No. 63-FZ of June 13, 1996 (as last amended on 29 June 2009), translation available at http://www.wipo.int/wipolex/en/text.jsp?file_id=202465.

523 Article 183, Criminal Code of the Russian Federation No. 63-FZ of June 13, 1996 (as last amended on 29 June 2009), translation available at http://www.wipo.int/wipolex/en/text.jsp?file_id=202465.

524 Civil Procedural Code of the Russian Federation No. 138-FZ of November 14, 2002 (as last amended on 6 February 2012).

525 Anna Grishchenkova, The Discovery Process in Russia. Will the New Era Come?, FBK Legal (June 2012) http://www.legal500.com/developments/20074.

526 Anna Grishchenkova, The Discovery Process in Russia. Will the New Era Come?, FBK Legal (June 2012) http://www.legal500.com/developments/20074 (citing Ruling of SAC of March 29, 2010 # BAC-3103/10; and Ruling of FAC of North-Caucasian district of October 29, 2007 # Ф08-7201/07).

527 Anna Grishchenkova, The Discovery Process in Russia. Will the New Era Come?, FBK Legal (June 2012) http://www.legal500.com/developments/20074.

528 Dmitry Maleshin, The Russian Style of Civil Procedure, 21 Emory Int'l L. Rev. 543, 548 - 549 (2007).

consequence, "some lawyers produce evidence . . . a matter of minutes prior to delivery of the judgment of the first instance court."[529]

c. Secrecy During Litigation

While the Russian constitution requires open court proceedings, in camera hearings are available in cases involving trade secrets to protect secrecy. News reports indicate that courts do grant such requests.[530]

6. Employee-Employer Relationships

Employees are obligated to keep trade secrets confidential. However, under the regime of commercial secrecy defined in Article 10 of the Commercial Secrecy Law, an employer must ensure that employees sign agreements and meet several other strict formalities described above. If the employer is able to meet these requirements, the employee's obligation lasts for so long as the trade secret remains a secret.531

There is some question as the remedy against a current or former employee who violates, or threatens to violate, a properly established trade secret. As discussed above, the Labor Code provides that such a violation is grounds for dismissal of the employee, the Civil Code provides for damages, and the Criminal Code provides for potential fines and jail sentences. The question is whether injunctive relief is available against the employee, which is, in practice, in doubt, as discussed above.

Neither civil nor labour law expressly address non-compete clauses in Russian employment agreements. One report states that they are becoming more common in Russian employment agreements.[532] On the one hand, if too restrictive, such clauses may violate Article 37 of the Russian Constitution, which guarantees freedom of labor.[533] On the other hand, Article 55 allows limitations on such rights to protect other interests recognized by law, and the law of commercial secrecy is protected under both the labor and civil codes.[534] Therefore, such clauses may be enforceable, although "no abundant court practice typical of many [other] countries" with respect to such clause "has yet been established."[535]

---

529 Anna Grishchenkova, The Discovery Process in Russia. Will the New Era Come?, FBK Legal (June 2012) http://www.legal500.com/developments/20074.

530 Court allows BP not to disclose information on Rosneft deal, http://www.rapsinews.com/judicial_news/20111010/256186687.html, 10 October 2011; Coal producer secures hearing for suit against antimonopoly service, http://www.rapsinews.com/judicial_news/20110930/255926069.html, 30 September 2011.

531 Russian Civil Code, Art. 1470(2).

532 Yury Ivanov, Non-Compete Clause in Russia: Do the Laws Compete?, The Moscow Times, 16 October 2008, http://www.themoscowtimes.com/business_for_business/article/non-compete-clause-in-russia-do-the-laws-compete/371717.html#ixzz2RnClzTM9.

533 Yury Ivanov, Non-Compete Clause in Russia: Do the Laws Compete?, The Moscow Times, 16 October 2008, http://www.themoscowtimes.com/business_for_business/article/non-compete-clause-in-russia-do-the-laws-compete/371717.html#ixzz2RnClzTM9.

534 Yury Ivanov, Non-Compete Clause in Russia: Do the Laws Compete?, The Moscow Times, 16 October 2008, http://www.themoscowtimes.com/business_for_business/article/non-compete-clause-in-russia-do-the-laws-compete/371717.html#ixzz2RnClzTM9.

535 Yury Ivanov, Non-Compete Clause in Russia: Do the Laws Compete?, The Moscow Times, 16 October 2008, http://www.themoscowtimes.com/business_for_business/article/non-compete-clause-in-russia-do-the-laws-compete/371717.html#ixzz2RnClzTM9.

7. Data Protection and Exclusivity

When Russia joined the World Trade Organization in 2012, it established data protection for regulatory information concerning drugs. Data submitted for purposes of registering a pharmaceutical cannot be transferred, disclosed, or used for business purposes or for state registration purposes by a third party for six years without the consent of the applicant.[536] This provision is applicable to applications after the date of entry into force of the protocol on Russia's accession to the WTO.

8. Complementary Legal Institutions

On the Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, Russia receives a score of 4.43 out of 10, which ranks it 92nd in the world.[537] It ranks particularly low with respect to judicial independence (2.66 out of 10) and impartial courts (2.88 out of 10), as well as protection of property rights (3.02 out of 10).[538]

9. Technology Transfer

There appear to be no express technology transfer provisions of consequence under Russian law.

536 IP Legislation News, http://www.gorodissky.com/law_news/?newsid=34, 21 August 2012.

537 Fraser Institute, Economic Freedom of the World 2012 Annual Report at 140 (2012).

538 Ibid.

South Africa

1. Overview

South African law is the product of a number of influences reflecting the country's unique history. It is largely founded on Roman Dutch law, but combines the additional influence of English common law, customary law, later statutory enactments, and the Constitution of 1996. In South Africa, there are no statutory laws of general applicability concerning trade secrets. Rather, the common law sanctions trade secret infringement pursuant to an unfair competition cause of action based on the Lex Aquilia, a Roman law concerning delicts or torts that compensated parties for damnum iniuria datum or "damage unlawfully inflicted." Further details are supplied below. There is significant and extensive case law on trade secrets in South Africa.

South Africa is undergoing an intellectual property law review process expected to result in reform:

> There is currently a review of the entire body of intellectual property law with a view to bringing it in line with international best practice, but also to align it with the strategic planning of Government. This review process, which was announced and commenced at the IP Indaba in August 2012, is closely linked to the drafting of an IP Policy instrument spanning the entire field of IP and its interfaces with other areas of law, and is expected to be continued during 2013. The IP Policy document will be a cross-cutting policy instrument, also taking into account international developments, and will be the outcome of an inclusive consultation process. It is likely to lead to amendments of all IP laws.[539]

2. Scope and Subject Matter

a. Definitions

South Africa's statutory law contains no general definition of trade secrets. However, numerous cases have defined the concept. A typical and oft-cited definition is as follows:[540]

> (1) "It must involve and be capable of application in trade or industry; that is: it must be useful."
>
> (2) "It must not be public knowledge and public property, that is objectively determined it must be known only to a restricted number of people or to a close circle."
>
> (3) "The information objectively determined must be of economic value to the person seeking to protect it."

The definition largely reflects international norms: the information must be commercial information, broadly understood; it must actually be secret; it must derive value from being secret; and the owner must take reasonable steps to safeguard secrecy. The last requirement of

539 Practical Law Company, IP in business transactions: South Africa overview (April 2013), http://uk.practicallaw.com/6-519-5891#a480193.

540 Advtech Resourcing (Pty) Ltd v Kuhn 2007(4) ALL SA 1386 ,C para51; see Bambelela Bolts (Pty) Ltd v Ball and Another (J 2977/11) [2012] ZALCJHB 148 (citing Advtech); Document Warehouse (Pty) Limited v Truebody and Another (2010/26977) [2010] ZAGPJHC 92 (13 October 2010) (citing Advtech).

"reasonable steps" is more implicit than explicit, but can be understood from the need to keep knowledge to a "restricted number" or "close circle."

b. Scope and Subject Matter Under Civil Law

South African courts interpret the subject matter of trade secret law broadly. Trade secrecy covers both confidential business information and technical information.[541] The information that is the subject of trade secrecy must not be in the public domain. Secrecy need not be absolute, but dissemination must be limited to parties with some obligation to keep the information secret.[542]

A leading treatise lists several examples of items of confidential information protected as trade secrets in South Africa. Technical information protected has included:

> "a tile-coating process (which was viewed as a unique process when taken as a whole); on-line sealing of leaks; manufacturing of fiberglass furniture; information concerning lifting devices; chemicals for the swimming pool industry; veterinary products; anti-freeze solution; fiber-glass products for agriculture; swimming pools and swimming pool cleaning equipment; and chemical formulae."[543]

The list of examples of confidential business information protected by South African courts is just as extensive:

> "a list of customers and a telegraphic code; a list of names of fruit farmers; the name and address of a manufacturer of a "multiwing fan"; confidential business information derived from stolen documents; information compiled by a trader in the exercise of his skill and labour; a list of employer's clients, together with their telephone and fax numbers; information concerning tender prices; a computer program concerning accounting and administrative systems for doctors; specialized sales techniques and trade connections; information useful in persuading a business to contract for consulting services; results of an evaluation and a list of topics to be studied compiled by an employee; a new label designed for a new wine; and information relating to an estate agent's business."[544]

As these extensive lists demonstrate, the subject matter covered by South African trade secret cases is broad and the precedent is ample.

To understand the scope and subject matter of trade secret law in South Africa, it is helpful to understand its origin as a cause of action for unfair competition based on the ancient Roman law, the Lex Aquilia. The Lex Aquilia imposes liability for wrongful acts that intentionally or negligently damage property.[545] The importance of this basis for trade secret liability in South Africa is that the Lex Aquilia provides a broader, more flexible basis for trade secret liability than English common law. Where the English common law focuses on breach of a fiduciary

541 MacLaren, Trade Secrets Throughout the Word, § 34.5 - § 34.6 (2012).

542 Ibid.

543 MacLaren, Trade Secrets Throughout the Word § 34.5 (2012) (citing cases).

544 MacLaren, Trade Secrets Throughout the Word § 34.6 (2012) (citing cases).

545 MacLaren, Trade Secrets Throughout the World § 34.4 (2012).

or contractual duty, the Lex Aquilia imposes liable for actions that are wrongful because they violate the "*boni mores* - the legal convictions of the community."[546]

As a consequence of its basis in the Lex Aquilia, trade secret protection in South Africa covers both misappropriation and breach of duty. An example of a misappropriation case is the seminal case of Dun and Bradstreet (Pty) Ltd v SA Merchants Combined Credit Bureau (Cape) (Pty) Ltd.[547] In that case the plaintiff and defendant were rival credit bureaus, and the defendant had illicitly obtained and resold the plaintiff's data. The defendant did not breach a duty to plaintiff. Rather, its liability was based on its wrongful act, with the court judging wrongfulness according to the standard of "fairness and honesty in competition."[548]

It is especially important that trade secrecy in South Africa has its basis in the Lex Aquilia because of the country's intermingled Dutch Roman law and English common law heritage. Several trade secret cases cite English precedent that states that a trade secret will be protected only if it is imparted to the defendant in confidence – i.e., only if there has been a breach of duty, rather than misappropriation.[549] One commentator who analysed this issue at length explains that this view is almost certainly incorrect.[550] The Lex Aquilia and the prior cases do not support it.[551] Moreover, statements that trade secrecy is based on a relationship appear to have been made in cases where there was a relationship, and thus misappropriation was not at issue.[552]

Courts also will likely impose a duty on a third party that receives information as a result of breach of duty by another, at least if the third party does so knowingly.[553]

c. Scope and Subject Matter Under Criminal Law

There are no criminal statutes in South Africa generally applicable to trade secrets.

3. Fault

a. Standard Under Civil Law

As described above, trade secret liability in South Africa can be based on either breach of duty or misappropriation. Breach of duty can arise from and express agreement – either a

546 Johann Knobel, Wrongfulness Of Trade Secret Misappropriation; and Trade Secrets As Objects Of Subjective Rights, 2000 Acta Juridica 196 (2000).

547 Dun and Bradstreet (Pty) Ltd v SA Merchants Combined Credit Bureau (Cape) (Pty) Ltd., (1968)1 SA 209.

548 Ibid at 218–19.

549 See, e.g., Meter Systems Holdings Ltd v Ventem (1993) 1 SA 409 (W) 426ff.

550 Johann Knobel, Wrongfulness of Trade Secret Misappropriation; and Trade Secrets As Objects Of Subjective Rights, 2000 Acta Juridica 196 (2000).

551 Johann Knobel, Wrongfulness of Trade Secret Misappropriation; and Trade Secrets As Objects Of Subjective Rights, 2000 Acta Juridica 196 (2000).

552 Johann Knobel, Wrongfulness of Trade Secret Misappropriation; and Trade Secrets As Objects Of Subjective Rights, 2000 Acta Juridica 196 (2000).

553 Dun and Bradstreet (Pty) Ltd v SA Merchants Combined Credit Bureau (Cape) (Pty) Ltd., (1968)1 SA 209, 218-19 ("a rival trader who is not a client but in some manner obtains this information and, well knowing its nature and the basis upon which it was distributed, uses it in his competing business and thereby injures the first mentioned trader in his business, commits a wrongful act vis-a-vis the latter and will be liable to him in damages.").

commercial or employment agreement, or an implied duty based on fiduciary responsibilities.[554] Situations in which implied duties arise include employment and certain commercial relationships.[555]

In a case of misappropriation, the question will be whether the defendant has committed an unlawful act. Such unlawful acts would include actions that are crimes or torts in and of themselves. However, as an action based on the Lex Aquilia, any act that violates the "*boni mores* - the legal convictions of the community" is an unlawful act.[556] While disruptive, but fair, competition is legal,[557] acquiring information by means that violate commercial morality (e.g., through commercial and industrial espionage), is likely to violate boni mores.

b. Criminal Law

There are no criminal statutes in South Africa generally applicable to trade secrets.

4. Remedies

a. Civil Law

The following remedies are available:

- Injunctive relief, both interlocutory and permanent, including ex parte injunctions and injunctions to eliminate the defendant's wrongful head start.[558]
- Seizure and destruction of infringing materials pursuant to an order for delivery up.[559]
- Monetary relief, either in the form of compensatory damages or recovery of defendant's profits.[560]

b. Criminal Law

There are no criminal statutes in South Africa generally applicable to trade secrets.

5. Procedures

a. Emergency Action to Preserve Proof

In South Africa, as in the United Kingdom, an ex parte procedure known as an Anton Piller Order is potentially available to plaintiffs seeking to preserve proof.[561] The procedure allows the plaintiff to apply directly to the court without informing the potential defendant. If granted, the plaintiff may search the defendant's premises and seize documents. The order allowing this procedure may be no more broad than is necessary to preserve the relevant evidence. An Anton Piller Order is granted at the discretion of the court upon a showing that it

554 MacLaren, Trade Secrets Throughout the Word § 34:20 (2012).

555 Ibid.

556 Johann Knobel, Wrongfulness Of Trade Secret Misappropriation; and Trade Secrets As Objects Of Subjective Rights, 2000 Acta Juridica 196 (2000).

557 Dun and Bradstreet (Pty) Ltd v SA Merchants Combined Credit Bureau (Cape) (Pty) Ltd., (1968)1 SA 209, 218-19

558 MacLaren, Trade Secrets Throughout the Word § 34:24 (2012).

559 MacLaren, Trade Secrets Throughout the Word § 34:24 (2012).

560 MacLaren, Trade Secrets Throughout the Word § 34:24 (2012).

561 MacLaren, Trade Secrets Throughout the Word § 34:24 (2012).

is necessary to preserve evidence. In South Africa, an official will conduct the search. As discussed in this paper's summary of UK law, Anton Piller orders have proven to be controversial in some cases.

b. Pre-Trial Discovery

In South Africa, pre-trial discovery is available but generally limited to documentary evidence under the supervision of the court.[562]

c. Secrecy During Litigation

In South Africa, procedures to safeguard the secrecy of plaintiff's confidential information are available during trade secret litigation. "Although the approach of 'South African' courts will normally be that there is a full right of inspection and copying, our courts have a discretion 'to impose appropriate limits when satisfied that there is a real danger that if this is not done an unlawful appropriation of [confidential information] will be made possible merely because there is litigation in progress and because the litigants are entitled to see documents to which they would not otherwise have lawful access.'"[563] Thus, protection is available, but limited greatly by the principle that defendant should have full access to evidence.[564]

6. Employee-Employer Relationships

Confidentiality obligations are generally enforceable, both before and after employment, whether express or implied.

Covenants not to compete are evaluated more carefully. Such restraints must be reasonable, and the Courts will look plaintiff's needs, public policy, and the need for the defendant to make a living before reaching a decision.[565] Courts will look at duration and geographic scope.

7. Data Exclusivity and Data Protection

South Africa currently provides no protection or exclusivity for data submitted for regulatory approval of pharmaceuticals or agricultural chemicals.

8. Complementary Legal Institutions

On the Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, South Africa receives a score of 6.98 out of 10, which ranks it 37th in the world.[566] It scores particularly low on legal enforcement of contracts (3.93 out of 10).

9. Technology Transfer

Outbound IP transfer agreements require registration and approval pursuant to a 2012 amendment to the Currency and Exchanges Act 9 of 1933.

---

562 International Civil Procedure, South Africa § 5.2 (2003).

563 Andre Vos, South Africa: Discovery of Confidential Documents, Mondaq (13 November 2008) at: http://www.mondaq.com/x/69448/Discovery+Of+Confidential+Documents.

564 Ibid.

565 MacLaren, Trade Secrets Throughout the Word, § 34:21 (2012).

566 Fraser Institute, Economic Freedom of the World 2012 Annual Report at 149 (2012).

Sweden

1. Overview

Sweden provides both civil and criminal law for trade secrets pursuant to the Act on the Protection of Trade Secrets[567] (Trade Secrets Act). The Trade Secrets Act provides protection that is broad in scope, with a wide set of remedies. The law is considered comprehensive and relatively effective. It offers Europe's most comprehensive set of statutory provisions dedicated to the protection of trade secrets.

Nevertheless, commentators do observe some deficiencies in the current Trade Secrets Act. A 2008 Legislative Committee report noted two deficiencies.[568] First, as discussed further below, the criminal provisions of the Act do not apply to a party that originally has lawful access to a secret—for example, an employee who discloses trade secrets. Second, the Act does not yet fully implement the EU Enforcement Directive to allow parties to seek an emergency search of an alleged infringer's premises to secure evidence.

Other observers have contended that the litigation process needs to be made more secure. A recent report prepared by the consultants for the EU contended that:

> The protection of trade secrets is insufficient in respect of information obtained by a party during court proceedings in general courts. A new rule on liability for damages should be added so that anyone who, without valid cause, discloses or commercially exploits trade secrets obtained in court proceedings may be liable for damages.[569]

2. Scope and Subject Matter

a. Definitions

Article 1 of the Trade Secrets Act defines "trade secrets" as follows:

> For the purposes of this Act, a "trade secret" means such information concerning the business or industrial relations of a person conducting business or industrial activities which that person wants to keep secret and the divulgation of which would be likely to cause a damage to him from the point of view of competition.[570]

Essentially, the definition of trade secrets in Sweden is similar to that found in most countries. Trade secrets consist of confidential business information that is actually kept confidential, and derives value from being kept secret.[571] Note that this definition applies to both the civil and criminal portions of the Trade Secrets Act.

---

567 Act on the Protection of Trade Secrets (SFS 1990:409).

568 Marianne Levin et al., Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, Sweden 13 (2010).

569 Hogan Lovells International LLP, Report on Trade Secrets for the European Commission, Appendix 3 at 63 (2012).

570 Article 1, Act on the Protection of Trade Secrets (Act 1990:409, of May 31,1990). English translation from Hogan Lovells International LLP, Report on Trade Secrets for the European Commission, Appendix 2 at 245 (2012).

571 Hogan Lovells International LLP, Report on Trade Secrets for the European Commission, Appendix 2 at 248 (2012).

b. Scope and Subject Matter Under Civil Law

Swedish trade secret law provides broad protection for confidential information. It covers both confidential business information and technical secrets.[572] Information can be tangible or intangible; it need not be reduced to writing.[573]

A leading treatise[574] compiled the following list of examples, which demonstrates the breadth of business information covered by Sweden's law, stating that trade secrets can include "specifications for a product not yet introduced to the market, information covering technical achievements, product test and sales data, and information covering commercial matters related to a business such as information covering administration, business planning, finance, and sales. Even information covering proposed ideas and projects are regarded as trade secrets if they otherwise meet the [definition]."[575]

Secrecy need not be absolute. It can be revealed to others, provided that access is limited and defined.[576] While a duty to keep information secret may be implied, those with access, particularly employees, must be informed that the information is intended to be kept secret.[577]

As discussed below, the law applies to both unrelated third parties (who may not misappropriate trade secrets) and parties with a contractual or other duty to the owner. The Trade Secrets Act makes a few express exceptions. It applies only to "unwarranted infringements" of trade secrets.578 Such unwarranted infringements do not include disclosure in the nature of whistleblowing (e.g., revealing criminal acts or public safety violations).[579] Nor do they include parties who acquire secrets in good faith—who do not know or have reason to know of infringement.[580]

The Trade Secret Act includes the requirement that there be a detriment to the owner in the very definition of trade secrets.[581] However, this requirement is tempered by the existence of liability for attempt, as discussed below. Thus, in most cases, there is likely to be either an attempt to take trade secrets or a sufficient detriment due to success in doing so.

c. Scope and Subject Matter Under Criminal Law

The Trade Secrets Act sanctions two types of criminal conduct. First, in Article 3 it sanctions business espionage, providing that "[a]nyone who wilfully and without authorization accesses a trade secret shall be sentenced for trade espionage."[582] Furthermore,

572 Article 1, Paragraph 2, Act on the Protection of Trade Secrets (Act 1990:409, of 31 May 1990). See MacLaren, Trade Secrets Throughout the World § 36:5 (2012).

573 Article 1, Paragraph 2, Act on the Protection of Trade Secrets (Act 1990:409, of 31 May 1990).

574 The list is quoted in its entirety from MacLaren, Trade Secrets Throughout the World § 36.5 (2012).

575 Ibid.

576 MacLaren, Trade Secrets Throughout the World § 36:5 (2012).

577 Ibid.

578 Article 2, Act on the Protection of Trade Secrets (Act 1990:409, of 31 May 1990).

579 Ibid.

580 Ibid.

581 Article 1, Act on the Protection of Trade Secrets (Act 1990:409, of 31 May 1990).

582 Article 3, Act on the Protection of Trade Secrets (Act 1990:409, of 31 May 1990). English translation from Hogan Lovells International LLP, Report on Trade Secrets for the European Commission, Appendix 2 at 245 (2012).

attempts and planning of trade espionage are also punishable under this Article. Second, in Article 4 it sanctions "unauthorized dealing," or tampering, with a trade secret, providing that "[a]nyone who obtains a trade secret knowing that the person who makes available the secret, or anyone before him, has accessed it through an act of trade espionage shall be punished for unauthorized dealing with a trade secret."[583]

The scope of criminal liability is thus broad (with a notable exception discussed below). So long as information meets the definition of a trade secret, then unauthorized access constitutes an act of criminal infringement. Moreover, the criminal liability continues through the transfer of possession of the secret, as parties who knowingly obtain trade secrets that were previously accessed without authorization are also liable.

There is, however, a limitation with respect to criminal liability. In a case involving Ericsson, an employee with authorization to access trade secrets disclosed them to an agent, who passed them to Russian agents.[584] The employee was not guilty under Articles 3 and 4, because those provisions sanction unauthorized access to the trade secret but not unauthorized disclosure, and the employee was authorized to access the trade secret. One report describes the case as follows:

> The judgment in the so-called Ericsson case (Svea Court of Appeals of 20 October 2003 in case B 5221-03) demonstrated deficiencies in the current rules. The case involved, among other things, an employee who had access to business secrets in his work and disclosed them to another person who in turn disclosed them to foreign intelligence agents. The prosecution of the employee for participating in grave corporate espionage was rejected, while the person who provided the details to the agents was sentenced to 8 years imprisonment for grave espionage. Apparently, the criminal responsibility under the Trade Secrets Act did not extend to also cover certain unauthorized disclosures and the use of business secrets effected by persons with lawful access to the secret, for example, employees.[585]

While a Legislative Committee recommended in 2008 that this issue be fixed, it has not yet been addressed.[586]

3. Fault

a. Standard Under Civil Law

The Trade Secret Act imposes civil liability for both accessing secrets without authorization and for using and disclosing them in breach of duty. In other words, civil liability is based on both grounds commonly used for trade secret liability: misappropriation and breach of duty. Civil liability for misappropriation under Article 5 of the Act is predicated on a violation of either Article 3 or 4, which address criminal liability. Articles 6, 7, add

583 Article 4, Act on the Protection of Trade Secrets (Act 1990:409, of May 31,1990). English translation from Hogan Lovells International LLP, Report on Trade Secrets for the European Commission, Appendix 2 at 246 (2012).

584 Marianne Levin et al., Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, Sweden 5 (2010).

585 Ibid.

586 Ibid at 13.

independent bases for civil liability based on breach of duty, while Article 8 covers third party liability. In whole, the Act contains the following bases for civil liability:

- Wilfully accessing trade secrets without authorization. (Article 3, via Article 5).
- Obtaining trade secrets with knowledge that they were previously wrongfully accessed. (Article 4, via Article 5).
- Intentionally or negligently exploiting or disclosing a trade secret without authorization, where that trade secret was learned in confidence in connection with a business transaction. (Article 6).
- Intentionally or negligently exploiting or disclosing a trade secret without authorization, where that trade secret was learned through employment. The employee must be informed it is secret and must know or ought know that he is not authorized to reveal it. (Article 7).
- Intentionally or negligently exploiting or disclosing a trade secret without authorization, where that trade secret was revealed due to a violation of Articles 3 – 7. (Article 8).

Liability for breach of duty does not require an express agreement. Duty can be imposed based "on professional standards of good conduct and trade customs" or professional duties of confidentiality. As detailed above, liability arises in the context of a business relationship, where a party learns of a secret in confidential circumstances (i.e. knows or has a reason to know that a confidence is being imparted). It also arises in the case of current employment (see below for further details).

Innocent third parties are excused from liability. A third party is innocent where they receive a trade secret in good faith, not knowing or having reason to know the secret was accessed or disclosed without authorization.[587]

b. Standard Under Criminal Law

The criminal portions of the Trade Secrets Act require intentional acts. Article 3 requires that the person wilfully access trade secrets without authorization. Article 4 applies to one who obtains trade secrets with knowledge that they were previously wrongfully accessed. "The word "obtains" is used to emphasize that it is not necessary for illegality that the perpetrator offer remuneration to the person providing the secret. It is sufficient, for example, that the discloser merely wishes to do the perpetrator a favor."[588] Consequently, and as is the case with respect to civil liability, there is no criminal liability if a person receives a trade secret in good faith.

4. Remedies

a. Remedies Under Civil Law

The following remedies are available:

- Injunctive relief, both interlocutory and permanent.[589]
- Seizure and destruction of infringing materials pursuant to an order for delivery up.[590]

587 Hogan Lovells International LLP, Report on Trade Secrets for the European Commission, Appendix 3 at: 59 (2012).

588 MacLaren, Trade Secrets Throughout the World § 36:8 (2012).

589 MacLaren, Trade Secrets Throughout the Word § 36:20 (2012).

- Compensatory damages in the form of out of pocket damages or, where those are difficult to calculate, then a damage award calculated to ensure that infringement is not profitable, considering factors such as defendant's profits.[591] Punitive damages are not available under Swedish law.[592]

b. Remedies Under Criminal Law

The following criminal penalties apply under the Trade Secrets Act:

- For wilfully accessing trade secrets without authorization: up to two years in jail, or six years in egregious cases (Article 3).
- For obtaining trade secrets with knowledge that they were previously wrongfully accessed: up to two years in jail, or four years in egregious cases (Article 4).

5. Procedures

a. Emergency Action to Preserve Proof

Currently, the Trade Secret Act contains no provision to secure evidence. A Swedish Legislative Committee recommended that such a provision be added in 2008, but it has not yet happened. Nevertheless, there are some provisions that can be used in this regard. If a criminal violation of the Trade Secrets Act is suspected, search and seizure by government officials is available.[593]

b. Pre-Trial Disclosure and Discovery

Swedish civil procedure provides limited pre-trial discovery. Documentary and physical evidence may be provided by court order at the request of one of the parties.[594]

c. Secrecy During Litigation

In Sweden, some procedures to safeguard the secrecy of plaintiff's confidential information may be available during trade secret litigation. The plaintiff can obtain closed or "in camera" hearings for both pre-trial procedures and the trial, and may seal the record. However, such requests are granted at the discretion of the court, at each stage of litigation (e.g., both trial and appellate).

As a consequence a party submitting its secret information to the Court can never be certain that the Court will indeed classify the information as secret. Also, even if a party requests the Court to take such an action at the same time as the information is

590 Ibid.

591 See Hogan Lovells International LLP, Report on Trade Secrets for the European Commission, Appendix 2 at 252 (2012) (discussing Article 9 of the Trade Secrets Act).

592 Marianne Levin et al. Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, Sweden at 8 (2010).

593 Marianne Levin et al. Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, Sweden 6 (2012).

594 Ibid.

submitted, it may take some time before the Court has decided on the question of secrecy and during that time the information is left open for inspection.[595]

6. Employee-Employer Relationships

Employees have a duty of loyalty during employment. Thus, under the Trades Secrets Act, an employee faces civil liability for using or disclosing trade secrets in breach of this duty. However, absent an express agreement, this duty ends upon termination of employment, except under exceptional circumstances. "According to Swedish courts an "exceptional case" is at hand if an employee gathers information during the employment with the intention to start a competing business when the employment has expired."[596]

Express agreements to keep secrets confidential after employment are normally valid and enforceable, but subject to scrutiny. A court will consider whether the agreement is equitable. However, if the provision is unlimited in duration, it may be considered inequitable and held void or modified.[597] Courts will also exclude knowledge that has become part of an employee's general skills and knowledge.[598]

Covenants not to compete are scrutinized carefully to determine whether they are inequitable.[599] Such agreements must be necessary and reasonable with respect to accomplishing their purpose. Factors to be considered include[600] the specific purpose to be accomplished, with protecting a trade secret (but not the employee's general skill and knowledge) as one of the permissible purposes. Duration and geographic scope are relevant to reasonableness as well.

7. Data Protection and Exclusivity

Sweden has implemented the standard EU approach to protection of test data for pharmaceuticals set forth in EU Directive 2001/83/EC as amended by EU Directive 2004/27/EC. This approach is known as the "8 + 2 + 1 year approach." Pharmaceutical test data submitted to government for new medicinal products and new indications or uses is protected from disclosure or use for 8 years. Once the 8 year period ends, the data can be used by generic manufacturers to prepare and apply for regulatory approval, but not market a product. This period of market exclusivity lasts 2 years. The initial applicant may receive another 1 year for new indications.

8. Complementary Legal Institutions

Sweden has a highly regarded commercial legal system that is among the most reliable and effective for contract and property rights enforcement. On the Fraser Institute Index of

595 Marianne Levin et al., Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, Sweden at 9 (2012).

596 MacLaren, Trade Secrets Throughout the World § 36:16 (2012).

597 MacLaren, Trade Secrets Throughout the World § 36:15 (2012).

598 Marianne Levin et al., Protection of Trade Secrets Through IP and Unfair Competition Law, AIPPI Report Q215, Sweden 3 (2012).

599 Ibid.

600 Judge Michaël Koch, Non-competition clauses in labour contracts, Sweden, Report for the XIVth Meeting of European Labour Court Judges (2006) available at: http://www.ilo.org/wcmsp5/groups/public/@ed_dialogue/@dialogue/documents/meetingdocument/wcms_159972.pdf.

Economic Freedom's component index for Legal System and Security of Property Rights, it receives a score of 9.2 out of 10, which ranks it 1st in the world.[601]

9. Technology Transfer

Sweden does not subject foreign investors to technology transfer requirements, joint venture technology contribution requirements, or license registration requirements.

601 Fraser Institute, Economic Freedom of the World 2012 Annual Report at 152 (2012).

United Kingdom

1. Overview

The United Kingdom[602] protects trade secrets almost exclusively pursuant to civil law under doctrines developed at common law. There are no statutes addressing trade secrets and no directly and generally applicable provisions in criminal law. While the protections that do exist are considered to be effective with respect to the subject matter they address,[603] there are notable uncertainties regarding scope, subject matter, and remedies. These limitations, together with the absence of criminal provisions, lead some commentators to describe UK trade secret protection as "relatively weak."[604] In recent decades, there have been a number of unanswered calls to strengthen UK trade secret law, including notable reports by the UK Law Commission (a statutory independent body) in 1981 that urged the adoption of a civil statute[605] and in 1997 that urged the adoption of a criminal statute.[606]

2. Scope and Subject Matter

All commercially valuable confidential information is potentially subject to trade secrecy protection. There may be some distinction between technical information (e.g. manufacturing diagrams or formulas) and non-technical business information (e.g. customer lists), as discussed below.

a. Definitions

Two leading cases supply the definition of trade secret under English law.[607] In *Coco v A.N. Clark (Engineers) Ltd.*, Megarry, J., stated:

> "In my judgment, three elements are normally required if, apart from contract, a case of breach of confidence is to succeed. First, the information must itself … 'have the

602 Strictly speaking, it is inaccurate to speak of UK law in this context, although it is frequently done. The UK's laws are governed by three jurisdictions: (1) England and Wales; (2) Northern Ireland; and (3) Scotland. England and Wales and Northern Ireland follow the common law, and commentators observe that the laws of the two jurisdictions regarding trade secrets are essentially the same. Hogan Lovells International LLP, Report on Trade Secrets for the European Commission Appendix 2 at 264. Scotland has a different legal system, with roots in both common law and Roman law. However, like other UK jurisdictions, Scotland has no express statutory provisions protecting trade secrets. Its law regarding trade secrets is not as developed, but is generally considered to be similar to the law of other UK jurisdictions. Hogan Lovells International LLP, Report on Trade Secrets for the European Commission Appendix 2 at 264.

603 Hogan Lovells International LLP, Report on Trade Secrets for the European Commission, Appendix 3 at 68.

604 Adrian Toutoungi, Trade Secrets Move (Slowly) Up the Agenda, Eversheds International Website, (16 August, 2012) available at: http://www.eversheds.com/global/en/what/articles/index.page?ArticleID=en/Industrial_engineering/Trade_secrets_move-slowly-up_the_agenda.

605 UK Law Commission, Report on Breach of Confidence (Law Com No.110), (October 1981).

606 UK Law Commission, Misuse of Trade Secrets Consultation Paper (November 1997) http://lawcommission.justice.gov.uk/docs/cp150_Legislating_the_Criminal_Code__Misuse_of_Trade_Secrets_Consultation.pdf.

607 See also Saltman Engineering Co. v. Campbell Engineering Co. Ltd. [1948] 65 RPC 203.

> necessary quality of confidence about it.' Secondly, that information must have been imparted in circumstances importing an obligation of confidence. Thirdly, there must be an unauthorised use of that information to the detriment of the party communicating it."[608]

In *Lansing Linde Ltd v Kerr,* Staughton L.J., further elaborated on this definition:

> ''What are trade secrets, and how do they differ (if at all) from confidential information? ... I would add first, that it must be information used in a trade or business, and secondly that the owner must limit the dissemination of it or at least not encourage or permit widespread publication.''[609]

In sum, a trade secret is information that:

1. Is used in business;
2. Has a confidential quality, and the owner has attempted to limit dissemination;
3. Was disclosed to the defendant under confidential circumstances; and
4. Defendant has used or disclosed the information (or threatens to do so) to the detriment of the owner.

b. Scope and Subject Matter Under Civil Law

Used in Business. Most commentators say that English law today treats as trade secrets both technical information and confidential business information.[610] However, there are cases that appear to cast doubt on this proposition. In *Faccenda Chicken Ltd. v. Fowler*, [1986] 1 All ER 617, the court held that a poultry business could not protect as secrets such items as customer lists, delivery routes, customer ordering habits, and prices. The reasoning excluded such confidential information from trade secret protection, indicating that this category is restricted to "secret processes of manufacture."

A later leading case, *Lansing Linde Ltd v Kerr,*[611] takes a broader view of trade secret protection. Butler-Sloss, LJ stated:

> "'Trade secrets' has, in my view, to be interpreted in the wider context of highly confidential information of a non-technical or non-scientific nature, which may come within the ambit of information the employer is entitled to have protected, albeit for a limited period."

Prior to *Lansing Linde,* however, English courts had rejected protection for "the names of agents; a report of a company's finances; staff names, aptitudes, specializations and characters; a company report; the value of a bid;" and, in two similar cases, a change bureau's "costs, profits and transaction numbers and values."[612] These cases indicate a court might reach the same conclusions, notwithstanding *Lansing Linde,* depending on the facts of the

608 Coco v. A.N. Clark Eng'rs Ltd., [1969] RPC 41.

609 Lansing Linde Ltd v Kerr, [1991] 1 W.L.R. 251.

610 For example, see Catherine Colston & Jonathan Galloway, Modern Intellectual Property Law 235 (2010 3d. ed).

611 [1991] 1 W.L.R. 251.

612 MacLaren, Trade Secrets Throughout the Word, § 39.18 (2010) (citing cases).

case. On the other hand, one leading commentator notes that cases after *Faccenda Chicken* appear to have abandoned that case's distinction between technical information and confidential business information, stating that "[t]his aspect of the *Faccenda Chicken* case seems to be almost a dead letter."[613]

Statements in case law regarding different treatment of technical information and confidential business information likely reflect a difference between the obligations of an employee with respect to information during and after his employment. While the law protects confidential information, there is a strong policy encouraging free movement of labor. This tension is resolved by distinguishing between the skill, knowledge, and experience that become part of an employee's professional expertise, on the one hand, and the employer's specific information on the other.[614] During employment, an employee has a broad duty to keep information confidential, whether there is an express agreement or not. After employment ends, however, Courts are reluctant to enforce even an express contractual obligation that would prevent an employee from using his general skill and knowledge, and even more reluctant to imply such an obligation in the absence of a written agreement.[615]

Some commentators and cases suggest that the distinction between knowledge an employee may use after leaving employment, and knowledge that an employee may not use, lies in the difference between objective and subjective knowledge set out by the House of Lords in Herbert Morris, Ltd. v. Saxelby, [1916] 1 AC 688. "A client list would fall into the [objective] category and thus be regarded as the employer's property even though it was in the departing employee's mind. It can be distinguished from the employee's own skills and aptitudes (even if developed in that employment) which would be that employee's subjective knowledge and not susceptible to protection by a restrictive covenant."[616] Unfortunately, as the same commentator concludes, "[t]hese are helpful guidelines, but considerable doubt remains as to the circumstances in which information may legitimately be protected."[617]

Confidential Quality. The information that is the subject of trade secrecy must not be in the public domain. Secrecy need not be absolute, but dissemination must be limited to parties with some obligation to keep the information secret.[618] Once information enters the public domain, at least through the fault of plaintiff, it generally ceases to be confidential.[619] There appears to be uncertainty with respect to both obligations and remedies where information becomes public through the action of the defendant or an innocent third party. This uncertainty is discussed in the remedy section below.

Disclosed to the Defendant Under Confidential Circumstances. To be confidential, the information must be communicated under conditions that create an obligation of confidentiality. A contractual relationship (in employment or commercial relationships) clearly creates such an obligation, although not all post-employment restrictions are enforceable, as discussed earlier. The more challenging and uncertain question is the

613 Gurry on Breach of Confidence: The Protection of Confidential Information, § 12.85 (2012).

614 Lancashire Fires Ltd. v. SA Lyons and Co. Ltd. [1996] FSR 629 at 674.

615 MacLaren, Trade Secrets Throughout the Word, § 39.30 (2010).

616 Employment Law in Practice § 5.8.1.3 (8th ed. 2008).

617 Ibid.

618 Coco v. A.N. Clark Eng'rs Ltd., [1969] RPC 41; Saltman Eng. Co. Ltd. v. Campbell Eng. Co. Ltd., [1968] 65 RPC 203; Exchange Telegraph Co. Ltd. v. Central News Ltd., [1897] 2 Ch. 48.

619 Mustad v. Allcock and Dosen, [1963] 3 All ER 416.

obligation of a party not bound by an express contractual provision that identifies the obligation of confidentiality. Most notably, the obligation of a third party that does not have any relationship with the trade secret owner, but that uses arguably improper means to obtain information – for example, a competitor that engages in economic espionage – is not entirely clear.

First, employees have a broad obligation to keep employer confidences while employed, even absent an express contract, and some (but less certain) obligation after employment as well. After employment, the obligation is more uncertain, but courts are willing to imply a term imposing an obligation to protect at least certain information as trade secrets. Even under the more restrictive view of Faccenda Chicken (discussed earlier) certain information classifiable as technical trade secrets would be protectable. However, even this obligation is not entirely clear, as indicated by AT Poeton (Gloucester Plating) v Horton, [2001] F.S.R. 169. There, the defendant had left employment setting up a competing business using the employer's confidential plating cell apparatus for electro-plating engines. His employment agreement lacked an express duty of confidentiality. The court refused to hold him liable, citing the lack of an express agreement, the policy allowing former employees to exercise skills and general knowledge, and his status as a junior employee. As one commentator notes "the dividing line between what is and is not protectable post-employment (whether or not express covenants exist) has [not] become any easier to discern and cases in this area are numerous despite frequent guidance from the courts."[620]

Second, in a commercial relationship, information disclosed during negotiations or other business relations is likely to be treated as confidential if it is clear that the information is provided in confidence. A leading case in this regard is Seagar v. Copydex Ltd., [1967] 1 W.L.R. 923, where an inventor disclosed his invention during the course of business negotiations that concluded unsuccessfully. The court found the conditions to be sufficient to impose an obligation of confidentiality because the defendant was made aware that the plaintiff considered the information confidential.

Third, and apparently most open to doubt, the obligation to keep information confidential may be inferred form circumstances. In 1981, the U.K. Law Commission issued a report calling for a civil trade secrets statute (as noted earlier, the commission called for a criminal trade secrets statute at a later date, in 1998).[621] One of the concerns that motivated the Commission's call for a statute was its uncertainty of the answer to the question: "Can information initially become impressed with an obligation of confidence by reason only of the reprehensible means by which it has been acquired?"

To be clear, this situation is different from one where a third party receives information from one (e.g. an employee) who has a duty to keep it confidential. Under such circumstances, if the third party recipient knows or later comes to know of the breach, they incur an obligation, even if their intent was innocent.[622]

The more uncertain situation is one in which the information is somehow obtained by a party who has no obligation or relationship with the owner of the information.

620 Jon Lang, The Protection of Commercial Trade Secrets, 10 E.I.P.R. 462, 470 (2003).

621 UK Law Commission, Report on Breach of Confidence (Law Com No.110), (October 1981).

622 Fraser v. Evans, [1968] 1 QB 39, 361. As Lord Denning, M.R. stated in Fraser v. Evans "even if he comes by it innocently, nevertheless once he gets to know that it was originally given in confidence, he can be restrained from breaking that confidence."

Notwithstanding the Law Commission's earlier concerns, it appears that courts are willing to find an obligation where a party obtains information by evading security measures. In *Creation Records Ltd v News Group Newspapers Ltd,* [1997] E.M.L.R. 444, the record label for the band Oasis was able to restrain publication of photographs of the set for the band's latest album cover. The court based the obligation on the fact that the newspaper photographer should have known that the scene was not public because of security measures around the scene. As one commentator noted, the recognition of a law of privacy appears to have made it easier for courts to recognize an obligation of confidentiality, thus putting into "doubt" the "strict relationship-based theory of breach of confidence."[623]

Use or disclosure of information to the detriment of the owner. It may be necessary for the owner to show that use or disclosure is likely to harm him, at least in order to receive an injunction.[624] In most instances such harm is likely to be present, but the requirement might prove problematic for a party that owns but does not use or intend to us information. (For example, information about the second-best way to manufacture a product, where the owner is already using the best method.)

c. Scope and Subject Matter Under Criminal Law

The UK's criminal law does not protect trade secrets. There are instances where a crime committed in the course of appropriating a trade secret might be punished. These instances include burglary, intercepting communication, unauthorized access to a computer, or conspiracy to defraud.[625] However, the underlying information is not the subject of criminal law. The case of *Oxford v. Moss*[626] illustrates this point. The defendant, an Oxford student, was prosecuted for stealing an exam answer before the test. He read and returned the answer paper. The court held that the defendant could not be charged with theft, as he had returned the physical paper and the *information* in the paper was not property under the Theft Act of 1968.

3. Fault

a. Standard Under Civil Law

Civil trade secrecy law in the UK does not frame the cause of action for trade secret in terms of fault, such as through intentional or negligent disclosure or wrongful appropriation. Rather, as discussed earlier, the offense is in using or disclosing the information in breach of a duty not to do so, regardless of whether the using or disclosing party intends to breach the duty or harm the claimant. Moreover, the requirement that a trade secret be disclosed to the defendant under confidential circumstances shifts the focus from whether the information was misappropriated, as the law requires in countries such as the United States, to whether the defendant had a duty not to disclose the information. As discussed above, however, UK courts have been willing to infer that the information was disclosed under confidential circumstances, and thereby create a duty not to disclose, where the defendant obtained the

623 Jon Lang, The Protection of Commercial Trade Secrets, 10 E.I.P.R. 462, 469 (2003).

624 Coco v. A.N. Clark Eng'rs Ltd., [1969] RPC 41.

625 Jon Lang, The Protection of Commercial Trade Secrets, 10 E.I.P.R. 462, 464 (2003).

626 (1979) 68 Cr.App.R. 183.

trade secret under circumstances where the owner indicated that the information was to remain private.[627]

b. Criminal Law

The issue of fault in criminal trade secrecy is irrelevant in the UK, due to lack of a criminal statute.

4. Remedies

a. Civil Law

The following remedies are available:

- Injunctive relief, both interlocutory and permanent.
- Monetary relief, either in the form of compensatory damages or recovery of defendant's profits.

Injunctive relief is not mandatory. If a defendant's actions effectively make the information public, then the information may no longer be confidential, thus precluding an injunction,[628] but not monetary remedies. In other cases, however, a defendant has been enjoined despite the fact that its actions made the information very public in both a brochure and patent application.[629] Alternately, defendant may be enjoined for a limited period to negate its improper "head start" in obtaining the information.[630]

b. Criminal Law.

Not applicable.

5. Procedures

a. Emergency Action to Preserve Proof

In the UK, an ex parte procedure known as an Anton Piller Order is potentially available to plaintiffs seeking to preserve proof. The procedure allows the plaintiff to apply directly to the court without informing the potential defendant. If granted, the plaintiff may search the defendant's premises and seize documents. The order allowing this procedure may be no more broad than is necessary to preserve the relevant evidence. An Anton Piller Order is granted at the discretion of the court upon a showing that it is necessary to preserve evidence. They have proven to be controversial in some cases, so they are not granted as a matter of routine, but rather must be fully justified by an extremely strong prima facie case and a need to preserve evidence from a real possibility of destruction or concealment.[631]

Another ex parte procedure is available, an "order for delivery up," which is less invasive than an Anton Piller Order. An order for delivery up does not authorize a search. Instead, the plaintiff may apply directly to the court without informing the potential defendant for an order

627 As one commentator noted, these cases cast "doubt" on the "strict relationship-based theory of breach of confidence." Jon Lang, The Protection of Commercial Trade Secrets, 10 E.I.P.R. 462, 469 (2003).

628 Attorney General v. Guardian Newspapers Ltd. (No. 2), [1988] 3 All ER 545. (Lord Donaldson, M.R.).

629 Speed Seal Ltd. v. Paddington, [1985] 1 WLR 1327.

630 Fisher Karpark Industries Ltd. v. Nichols, [1982] FSR 351.

631 MacLaren, Trade Secrets Throughout the Word, § 39.34 – 39.35 (2010).

to deliver up certain documents to the plaintiff or his representative.[632] As with an Anton Piller Order, the plaintiff must show that the order is necessary to preserve evidence.

b. Pre-Trial Discovery

In the UK, pre-trial discovery is available (it is referred to as "disclosure.") Disclosure is limited to documentary evidence.

c. Secrecy During Litigation

In the UK, procedures safeguard the secrecy of plaintiff's confidential information during trade secret litigation. The plaintiff can obtain closed or "in camera" hearings for both pre-trial procedures and the trial.

6. Employee-Employer Relationships

As discussed above, UK law makes a distinction between the duties of current and former employees with respect to confidential information. During employment, an employee's obligations are broad, even absent an express contract. After employment, courts take a more restrictive view. In circumstances involving important confidential information, a court may enforce a duty, even in the absence of an express contract. However, in other circumstances, even where there is an express confidentiality clause or non-compete agreement, a court may choose not to enforce it. As discussed in greater detail above, the guiding policy consideration is to allow former employees to exercise skills and general knowledge so as not to impede employment prospects. However, the law on this point often difficult to discern.[633]

7. Data Exclusivity and Data Protection

The UK has implemented the standard EU approach to protection of test data for pharmaceuticals set forth in EU Directive 2001/83/EC as amended by EU Directive 2004/27/EC. This approach is known as the "8 + 2 + 1 year approach." Pharmaceutical test data submitted to government for new medicinal products and new indications or uses is protected from disclosure or use for 8 years. Once the 8 year period ends, the data can be used by generic manufacturers to prepare and apply for regulatory approval, but not market a product. This period of market exclusivity lasts 2 years. The initial applicant may receive another 1 year for new indications.

8. Complementary Legal Institutions

The United Kingdom is generally regarded as having a commercial legal system that is among the most reliable and effective for contract and property rights enforcement. On the Fraser Institute Index of Economic Freedom's component index for Legal System and Security of Property Rights, the UK receives a score of 8.74 out of 10, which ranks it 11th in the world.[634]

9. Technology Transfer

The UK does not subject foreign investors to technology transfer requirements, joint venture technology contribution requirements, or license registration requirements.

632 MacLaren, Trade Secrets Throughout the Word, § 39.36 (2010).

633 Jon Lang, The Protection of Commercial Trade Secrets, 10 E.I.P.R. 462, 470 (2003).

634 Fraser Institute, Economic Freedom of the World 2012 Annual Report at 165 (2012).

United States

1. Overview

In the United States, the law of trade secrets is well developed and quite strong. The civil law of trade secrets is governed by the law of each American state, while national law addresses criminal trade secret theft with the Economic Espionage Act (with additional criminal statutes in some states). This section will summarize general principles of US trade secret law, while noting certain particularly significant deviations from the norm.

Summarizing the US law of trade secrets presents a challenge because of the United States' federalist system of governance. This system leaves many important legal matters, including the civil law of trade secrets, to the jurisdiction of the US's fifty states. This system of federalism creates great legal diversity among the states, but that diversity is not as pervasive as outside observers may believe at first glance. There is considerable convergence in US state law generally, and with respect to trade secrecy particularly. Almost all of the fifty states have adopted a model law -- the Uniform Trade Secrets Act (UTSA), albeit with some variations.

US trade secret law is among the strongest and best-developed bodies of trade secret law in the world. With a history of development at common law stretching back to the 19th Century, development of model laws throughout the 20th Century, and then extensive and frequent judicial interpretation of those laws, the US law of trade secrets has been afforded ample opportunity to develop. The system includes effective remedies and well-developed procedures for enforcing and trade secrets and protecting them during litigation. As in other jurisdictions, there are some restrictions on post-employment enforcement that would deprive former employees of the ability to exercise their skills to make a living. Finally, while the US legal system is consistent and generally reliable, it also considered expensive.

US Federalism and Trade Secrets

A brief note on the US system of federalism and the manner in which it affects the law is necessary because trade secret law is largely state law in the US (unlike copyright, patent and trademark law, which are largely or exclusively matters of federal law). This federalist system creates a dual system of government, with both state and federal court systems. As the system has evolved in practice, there are some areas where each level has exclusive or nearly exclusive jurisdiction (e.g. contract and tort law are largely state matters) and certain areas of shared jurisdiction (e.g. large areas of criminal law).

The United States' federalist structure of government thus leaves many important legal matters, including the law of trade secrets, to the jurisdiction of the fifty states. This system creates legal diversity at the level of state law, with fifty different legislatures and court systems making law.

Nevertheless, diversity in US state law is not as great as outside observers may believe at first glance. There are four primary forces leading to a large (but never complete) degree of convergence among US laws and their effects on commercial parties:

(1) the common law system, which permits judges to aid the development of law by following decisions of other states' courts;

(2) a very successful movement to develop model rules of law and model statutes to encourage greater uniformity and predictability in state law;

(3) commercial activity is somewhat concentrated in certain large states (e.g. New York, California, Illinois, Texas and Florida); and

(4) commercial parties often attempt to reduce legal unpredictability by contracting for choice of law provisions that indicate state law that is well-developed and well-regarded by the parties.

As a result of this convergence, there is a broad degree of predictability and uniformity in the laws that a commercial party faces in the United States. One can thus arguably make meaningful statements about the content of US law and its effect on the costs and incentives facing US businesses.

Still, one should note that state laws often differ in certain important respects. Legislatures may adopt model laws with small deviations (or later amend or contradict them). A particular state's courts may adopt a unique interpretation of a model law, or distinguish or deviate from widely-accepted common law principles. A commercial party may find that it is unable to choose its preferred state law on a particular issue for a variety of practical and legal reasons.

Trade secrecy law in the United States follows the pattern of convergence described above. Since the early Nineteenth Century, state courts in the United States have recognized trade secret protection as common law under widely similar principles. In the early Twentieth Century, the American Law Institute's influential Restatement of Torts helped clarify and shape the principles of common law protection.[635] Finally, in 1979 the National Conference of Commissioners on Uniform State Laws adopted the Uniform Trade Secrets Act, a model law recommended for adoption by the states. (State legislatures are under no obligation to adopt model laws and, indeed, some such model laws are far more successful than others).

As of this writing, 47 out of 50 states and the District of Columbia[636] have adopted the Uniform Trade Secrets Act. The three exceptions are New York, North Carolina and Massachusetts. These three exceptions to the adoption of the UTSA are significant, because of their size, commercial importance, and concentration of technology industries, but they do provide extensive trade secret protection. North Carolina has its own act that is similar to the UTSA in many respects. New York and Massachusetts follow common law principles largely similar to the UTSA. As of this writing in mid-2013, Massachusetts is considering adoption of the UTSA, while Texas became the 48th state to adopt the UTSA earlier this year.[637]

With respect to the criminal law of trade secrets, both national and state laws exist. Over 25 states have criminal trade secret laws.[638] These laws apply in addition to, and are not pre-empted by, the federal Economic Espionage Act of 1996. The state laws criminalize intentional misappropriation of trade secrets.

It is thus possible to generalize about the law of trade secrets in the United States, but some caution is warranted. On the one hand, the nearly universal adoption of the UTSA has created a largely uniform body of law. On the other hand, each state is free to deviate from the UTSA and the remaining states that have yet to adopt the UTSA are populous states with significant

635 First Restatement of Torts § 757 (1939).

636 The District of Columbia, the seat of the national government comprising the city of Washington, is a separate jurisdiction, not located in a state.

637 For updates on adoption of the Uniform Trade Secrets Act, see Uniform Law Commission, Trade Secrets Act http://uniformlaws.org/Act.aspx?title=Trade%20Secrets%20Act .

638 Melvin Jager, Trade Secrets Law, Appendix L (2012).

business activity. In the case of criminal law, the Economic Espionage Act creates a uniform body of national law, but state laws also co-exist with the federal Act. However, the state laws typically define trade secrets in essentially the same manner as the UTSA. While there are differences among US states, the large degree of uniformity and similarity among the states' laws allows this paper to describe a US law of trade secrets in broad, general terms, which is necessary and appropriate for this project.[639] The following discussion will thus summarize US trade law as much as possible, noting significant points of disagreement where relevant.

2. Scope and Subject Matter

a. Definitions

US trade secret law defines trade secrets broadly, covering both confidential business information and technical information. The UTSA defines trade secret as follows:[640]

> "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.

The federal criminal statute, the Economic Espionage Act, contains essentially the same definition of trade secrets as the UTSA – in fact, the language is identical in some parts. It contains an even more expansive list of examples than the UTSA, stating that "trade secret"

> "means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing."[641]

Before the development of the UTSA, the law of trade secrets had already been the subject of an earlier attempt to encourage uniform law in the First Restatement of Torts (1939). The Restatements were (and continue to be) an attempt to distil and restate principles from the common law in order to clarify and harmonize various fields of law.[642] Restatement of Torts

---

639 Nevertheless, the variance is sufficient to justify comparative legal studies and to allow econometric analysis of varying economic outcomes associated with those variations. See, e.g., Ivan Png, *(2012), Law and Innovation: Evidence from State Trade Secrets Laws, mimeo, National University of Singapore, SSRN; Ivan Png, "Trade Secrets, Non-Competes, and Mobility of Engineers and Scientists: Empirical Evidence", mimeo, National University of Singapore, SSRN; Michael* Risch, (forthcoming, 2012), "An Empirical Look at Trade Secret Law's Shift from Common to Statutory Law," in S. Balganesh (ed.), *Intellectual Property and the Common Law*. Cambridge University Press, Cambridge, UK.

640 Uniform Trade Secrets Act § 1 (available at: http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf).

641 18 USC § 1839(3).

642 It is widely acknowledged that the Restatements have often gone beyond mere description to attempt, with some success, prescription that influences the course of judicial decision-making.

Section 737, comment b, set forth six factors that courts continue to cite when determining whether information qualifies as a trade secret:

- The extent to which the information is known outside the claimant's business
- The extent to which it is known by employees and others involved in the business
- The extent of measures taken by the claimant to guard the secrecy of the information
- The value of the information to the business and its competitors
- The amount of effort or money expended by the business in developing the information
- The ease or difficulty with which the information could be properly acquired or duplicated by others

In sum, the US definition of trade secrecy is similar to that found in most jurisdictions, albeit with fewer complications, qualifications, or ambiguities. Trade secrets are (1) information that is used in a business, (2) that derives economic value from secrecy; and (3) that is actually confidential, and for which the business has taken reasonable steps to maintain confidentiality.

b. Scope and Subject Matter Under Civil Law

Secrecy need not be absolute. As the US Supreme Court stated in *Kewanee Oil Co. v. Bricron Corp.*,

> The necessary element of secrecy is not lost … if the holder of the trade secret reveals the secret to another "in confidence and under an implied obligation not to use or disclose it."… These others may include those of the holder's employees to whom it is necessary to confide it, in order to apply it to the uses for which it is intended…. Often the recipient of confidential knowledge of the subject of a trade secret is a licensee of its holder.[643]

A trade secret owner may make limited disclosure of its secrets to further its economic interests, provided that a substantial element of secrecy remains. In a leading case, *Metallurgical Industries, Inc. v. Fourtek, Inc.*,[644] the court held that secrecy was not lost when the owner disclosed secrets to a licensee and a potential business partner, even in the absence of an express agreement. The circumstances made it clear that the information was intended to remain secret and the parties had a mutual interest in keeping it secret.

The owner of a trade secret must make reasonable efforts to maintain secrecy. The level of effort required varies according to the value of the secret and the circumstances of the case. In a leading case, *Rockwell Graphic Systems, Inc. v. DEV Industries Inc.*,[645] Judge Richard Posner set forth the standard for determining whether efforts are reasonable. This approach weighs the costs of security measures versus the additional security benefit it provides, in light of the value of the trade secret. The more valuable a secret and effective the security measure, the more reasonable it is to incur the cost to apply it. The converse is true as well – a party need not incur high costs to protect low value trade secrets, or to employ measures with limited efficacy (unless the value of the trade secret is high).

643 Kewanee Oil Co. v. Bricron Corp., 416 U.S. 470, 475 (1974).

644 Metallurgical Industries, Inc. v. Fourtek, Inc., 790 F.2d 1195 (5th Cir. 1986).

645 Rockwell Graphic Systems, Inc. v. DEV Industries Inc.,925 F.2d 174 (7th Cir. 1991).

c. Scope and Subject Matter Under Criminal Law

Since the definition of trade secrecy is the same under both the Economic Espionage Act and the UTSA, the scope and subject matter of criminal and civil protection is largely the same. The comparative advantages of a criminal prosecution are the investigatory and sanctioning powers of criminal authorities, such as grants of immunity in exchange for testimony and (under certain circumstances) wiretapping.

Criminal law is more effective than civil law in addressing acts in the nature of economic espionage (thus the name of the federal statute). For a private party, civil law has relatively sufficient tools to investigate and pursue a suit against "ordinary" trade secret misappropriation – i.e. where a known party such as a former employee or business partner attempts to use a secret to set up competition. On the other hand, in cases where third parties, particularly foreign companies beyond the easy reach of civil law, conspire to steal a trade secret, criminal investigatory powers are useful. Such was the case in *United States v. Hsu*, 155 F.3d 189 (3d Cir. 1998), where agents of a company based in Chinese Taipei attempted to steal trade secrets regarding the manufacture of the cancer drug Taxol from Bristol-Myers Squibb. The Federal Bureau of Investigation used undercover agents and other criminal investigatory techniques over the course of 14 months, including a staged meeting with a Bristol-Myers Squibb employee playing a "corrupt scientist," to investigate and document the conspiracy to appropriate trade secrets.

State criminal laws are also essentially the same as the UTSA and the Economic Espionage Act with respect to scope and subject matter. One commentator has noted that courts are more cautious with respect to the requirement of secrecy in a criminal case than they are in a civil case because of the graver consequences in criminal cases.[646]

3. Fault

Under US law, a party is liable only if it intentionally misappropriates a trade secret. However, the category of acts constituting misappropriation is relatively large. For civil liability, under the UTSA, the key is whether the trade secret was obtained by "improper means" generally, while the Economic Espionage Act contains a specific list of acts essentially constitute improper means of obtaining a trade secret.

a. Civil Law

The Uniform Trade Secrets Act provides a remedy against "misappropriation" of trade secrets. The UTSA defines misappropriation as follows:

"Misappropriation" means:

(i) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or

(ii) disclosure or use of a trade secret of another without express or implied consent by a person who

(A) used improper means to acquire knowledge of the trade secret; or

646 Melvin Jager, Trade Secrets Law § 4.4 (2012). See, for example, United States v. Lange, 312 F.3d 263, 266 (7th Cir. 2002), which carefully examines the extensive measures that the trade secret owner took to keep the information secret.

(B) at the time of disclosure or use, knew or had reason to know that his knowledge of the trade secret was

(I) derived from or through a person who had utilized improper means to acquire it;

(II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or

(III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or

(C) before a material change of his [or her] position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.

Thus, misappropriation includes acquisition, use, or disclosure of a trade secret that was acquired (directly or indirectly) by "improper means." It also includes disclosure or use of a trade secret acquired by accident or mistake, provided that the party knows it is a trade secret before they are prejudiced by a change in position (e.g. expenditure of funds).

The key to this definition is the meaning of "improper means," a term that is broadly defined but subject to certain clear limitations. The UTSA defines "improper means" to include "theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means."[647] Improper means clearly include both crimes and torts, but the meaning of the term is much broader than that.

The breadth of the meaning of "improper means" is demonstrated by the seminal case of *E.I. DuPont deNemours & Co. v. Christopher*.[648] In that case, the defendants were photographers who were hired by an unknown party to take aerial photos of a chemical plant under construction. In other words, the defendants took the extraordinary measure of hiring an airplane to circle a construction site while they took photos. The trial court enjoined defendants and the appellate court affirmed. The appellate court observed that improper means extend beyond overt wrongful acts to cover various forms of economic espionage, depending on the facts and circumstances of each case. In this instance, the court justified its holding that the aerial photography constituted improper means on two grounds: (1) it violated commercial morality; and (2) it was an unforeseeable attempt to circumvent reasonable attempts to maintain secrecy.

Christopher's second ground for an expansive understanding of improper means – circumvention of reasonable attempts to maintain secrecy – has proven to be the more reliable to apply. At its heart is a cost-benefit analysis. A trade secret owner is required to take measures commensurate with the value of the trade secret, but it need not "guard against the unanticipated, the undetectable, or the unpreventable methods of espionage now available."[649] The court further stated "[r]easonable precautions against predatory eyes we may require, but an impenetrable fortress is an unreasonable requirement, and we are not disposed to burden industrial inventors with such a duty in order to protect the fruits of their efforts."[650]

Improper means is not, however, a concept without limitations. The comments to the UTSA list several proper means for discovering a trade secret: (1) independent invention; (2) reverse engineering; (3) observation from public use or display; (4) review of published

647 Uniform Trade Secrets Act § 1(1).

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

649 E. I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1016 (5th Cir. 1970).

650 E. I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1017 (5th Cir. 1970).

literature. Of these limitations, arguably the most legally significant is the allowance of reverse engineering.

b. Criminal Law

Under Section 1832 of the Economic Espionage Act, theft of trade secrets occurs where a party:

with intent to convert 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, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates or conveys such information;

(3) receives, buys or possesses such information, knowing the same to have been stolen or appropriated, obtained or converted without authorization;

(4) attempts to commit any offense described in paragraphs (1) through (3); or

(5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy... .[651]

There are five notable aspects to this definition: First, it requires that the misappropriation be intentional, both with respect to the intent to "convert a trade secret" and the act itself. Second, the act must be done with the intent or knowledge that it will "injure any owner of that trade secret." Third, the offenses covered are broad, ranging from stealing the information to copying or transmitting it without authorization. Fourth, it covers both attempted and actual trade secret theft. Fifth, it criminalizes receipt of trade secrets with knowledge that the trade secret was stolen as well as conspiracy to commit trade secret theft.

The US Congress recently expanded and clarified the scope of the Economic Espionage Act with the Theft of Trade Secrets of 2012.652 The new law ensures that the definition of trade secrets under the Act includes secrets related to both products and services that are used or intended for use in interstate or foreign commerce. Previously the language of the Act applied only to *products* produced or placed in interstate commerce. A 2012 decision of the US Court of Appeals for the Second Circuit reversed the conviction of a former Goldman Sachs employee who had stolen a computer program that was used internally at the firm, as the secrets related only to services provided by the firm, rather than a product that it sold.[653] The US Congress moved promptly to close what one sponsor of the bill called "a dangerous loophole."[654]

651 18 USC § 1832 (2013).

652 S. 3642, 112th Cong. (2012).

653 United States v. Aleynikov, 676 F.3d 71, 75 (2d Cir. 2012).

654 158 Cong. Rec. H6849 (daily ed. 18 December 2012) (statement of Rep. Smith).

4. Remedies

US law provides a comprehensive and strong set of remedies for violations of trade secrets. Criminal sanctions are strong, and the full array of civil remedies is available.

a. Civil Law

The UTSA provides for a full array of remedies. These remedies are typical in US law, and are routinely granted, provided that standards are met and proof is sufficient.

Pursuant to section 2, a plaintiff may receive both a preliminary and permanent injunction. No injunction is truly permanent, however, as it will be dissolved once the trade secret becomes public. However, "the injunction may be continued for an additional reasonable time period in order to eliminate commercial advantage that otherwise would be derived from the misappropriation."[655] In exceptional circumstances, a defendant may be required to pay only a royalty – those circumstances exist where the defendant innocently received the information and changed its position prejudicially without knowledge of the trade secret violation (e.g., invested in manufacturing capacity).[656]

A plaintiff may also recover damages. Available damages include plaintiff's actual losses and defendant's unjust enrichment (the portion not accounted as part of plaintiff's loss).[657] Alternatively, damages may be measured in terms of a reasonable royalty.[658] Finally, a plaintiff may receive exemplary (i.e., punitive) damages for wilful infringement of up to twice the amount of other damages awarded.[659] In exceptional circumstances, a court may award the prevailing party reasonable attorney's fees if its opponent acted in bad faith (under the usual rule in the United States, each party pays its own legal costs).[660]

b. Criminal Law

The primary national criminal law regarding trade secrets, the Economic Espionage Act, provides for both significant fines and prison time as sanctions. It distinguishes between trade secret theft performed for foreign governments (and government owned or controlled corporations) and trade secret theft performed for competitors.

In the case of trade secret theft performed for the "benefit any foreign government, foreign instrumentality, or foreign agent," an individual may receive up to a USD 5 million fine and up to a 15 year prison sentence, or both. In the case of an organization, it may receive a fine of up to USD 10 million or "3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided."

In the case of more ordinary trade secret appropriation, such as between firms, the Economic Espionage imposes slightly less stringent penalties. It provides that individuals can receive up to a 10 years prison sentence or a fine (the amount is unspecified).[661] Organizations

655 UTSA § 2.

656 UTSA § 2.

657 UTSA § 3.

658 UTSA § 3.

659 UTSA § 3.

660 UTSA § 4.

661 18 U.S.C. § 1832(a).

can be fined up to USD 5 million.[662] The Economic Espionage Act's criminal penalties also apply to both attempted offenses and conspiracies to commit offenses.[663]

5. Procedures

Extensive and routine procedures are available to protect trade secrets from public disclosure or misuse by the opposing party. There is no absolute privilege to protect evidence relevant to the case from disclosure to the opposing party, but a court's protective order will provide a basis for punishing any misuse or disclosure of trade secrets.

a. Emergency Action to Preserve Proof

Rules of civil procedure in the United States at both the national and state levels allow parties to seek ex parte seizure and impoundment orders to preserve evidence, including in trade secret cases.[664] However, such orders are not granted as of right, nor are they granted routinely. For example, in *First Technology Safety Systems, Inc. v. Depinet,*[665] the appellate court reversed the trial court's ex parte seizure and impoundment order in a trade secret case. The trial court had erroneously based its decision on the belief that electronic recordkeeping has generally made records easier to destroy, rather than any indication of a risk of concealment or destruction raised by that particular defendant or case. As this case demonstrates, such orders are not to be treated as routine and will only be granted in exceptional cases.

By contrast, in criminal cases, ex parte search and seizure orders are routine. Investigators must show probable cause and obtain a warrant from a judge allowing such an action, but cases under the Economic Espionage Act frequently include such procedures. This feature of the Economic Espionage Act, along with other procedures that protect confidentiality make it attractive to companies to refer matters to federal prosecutors. As one commentator notes "federal prosecutors may have more success at protecting the victim's confidential information than a potentially less-sympathetic plaintiff in a civil action."[666]

b. Pre-Trial Discovery

Pre-trial discovery is extensive in the United States in both civil and criminal matters. It likely is the most extensive system of discovery and disclosure in the world. The parties can request and receive documents, physical evidence, pose written questions, conduct depositions, and other procedures to gather evidence. The opposing party is required to cooperate or may be compelled to do so.

c. Secrecy During Litigation

US law provides extensive procedures for protecting trade secrets (and other confidential information) during litigation. A party may request that disclosure and discovery of trade

662 18 U.S.C. § 1832 (b).

663 18 USC 1832(a) and 18 USC 1831(a).

664 Rule 65 of the Federal Rules of Civil Procedure sets forth the standard.

665 11 F.3d 641 (6th Cir. 1993).

666 Douglas Nemec and Kristen Voorhees, Recent amendment to the Economic Espionage Act extends protection against misappropriation, Thomson Reuters New& Insight (13 February 2013), http://newsandinsight.thomsonreuters.com/Legal/Insight/2013/02_-_February/Recent_amendment_to_the_Economic_Espionage_Act_extends_protection_against_misappropriation/.

secrets be limited and that evidence and testimony be heard by the court in non-public hearing. Courts routinely grant such requests pursuant to a protective order – for example, as provided under Federal Rule of Civil Procedure 26(c). Generally, there is no absolute privilege to prevent disclosure of a trade secret that is relevant to proving a case.[667] However, the protective order will limit its use to preparation of the case, prevent disclosure in the public record or open court, and will serve as a basis for heavily sanctioning any party or attorney who discloses or uses the trade secret outside the scope of the protective order.

A trade secret claim must be pled with specificity – the standard in Federal court is "reasonable particularity."[668] As noted above, there is no privilege to completely withhold trade secrets, and a plaintiff must make clear the basis of its cause of action. Courts thus will often require plaintiffs to provide lists of trade secrets at issue at the beginning of litigation.[669] However, courts will protect trade secrets by allowing such lists and any other particularly sensitive portions of the complaint to be submitted under seal and protected pursuant to a protective order.[670]

In criminal trade secrets cases, both the indictment and the entire case file may be sealed, which prevents public disclosure and availability.[671]

6. Employee-Employer Relationships

Employees are generally under an implied duty not to disclose employer's confidential information both during and after employment. Generally, there are no significant limitations on confidentiality agreements.[672]

By contrast, the treatment of non-competes is much more varied.[673] This is the greatest source of state-to-state variation of the provisions discussed in this report. Some states expressly prohibit non-competes. Other states view them very skeptically, while still others view them more favorably. In substantially all instances where non-compete agreements are allowed, courts examine them to determine whether they are reasonable with respect to business necessity, duration, and geographic scope.

7. Data Protection

The United States provides five years of data exclusivity from marketing approval of a new chemical entity.[674] During that five year period, the FDA cannot accept or approve a

667 "There is no privilege excepting trade secrets from discover, but 'courts must exercise discretion to avoid unnecessary disclosures of such information." Dura Global Techs., Inc. v. Magna Donnelly, Corp., No. 07-cv-10945, 2007 WL 4303294, at *2 (E.D. Mich. 6 December 2007).

668 L-3 Communications Corp. v. Jackson Engineering & Maintenance, Inc., No. 10-cv-02868-MSK-KMT (D. Colo. 12 October 2007) (denying plaintiff's motion to compel discovery because it had failed to sufficiently identify the trade secrets at issue in its pleadings).

669 Ibid.

670 Ibid.

671 Tim Reagan & George Cort, Sealed Cases in Federal Courts, 20 (Federal Judicial Center 2009), http://www.fjc.gov/public/pdf.nsf/lookup/sealcafc.pdf/$file/sealcafc.pdf.

672 Melvin Jager, Trade Secrets §13.3 (2012).

673 Melvin Jager, Trade Secrets §13.4 (2012).

674 21 U.S.C. § 355.

competitor's application for an equivalent product based on data submitted by the first company.

The United States also provides three years of data exclusivity for test data where a company submits new test data to obtain approval for certain changes to a drug product, which may include new dosage forms, new indications, and a change from prescription to over-the-counter.[675] During this period, and in contrast to new entities, the FDA may take applications from competitors based on the test data and start the review process, but may not approve the application until the three years expires.

The United States provides a separate period for biologics, which are medical treatments derived from living organisms. Biologics are defined as treatments consisting of "a virus, therapeutic serum, toxin, antitoxin, vaccine, blood, blood component or derivative, allergenic product, or analogous product ... applicable to the prevention, treatment, or cure of a disease or condition of human beings.[676] They consist of a large (20% as of 2008) and growing segment of the drug market.[677] Biologic products are entitled to 12 years of exclusivity. Applications for biosimilar products may be submitted four years after licensing of the reference product, but may not be approved until 12 years following licensing of the reference product.[678]

Agrochemicals also receive a data exclusivity period. This period lasts for ten years with respect to data submitted to the Environmental Protection Agency to obtain regulatory approval of a new active ingredient (no approval of applications based on the originator's data).[679] In addition, the original registrant is entitled to an additional five years during which the second user must pay compensation to use the originator's data.[680]

8. Complementary Legal Institutions

The United States is generally regarded as having a commercial legal system that is among the most reliable and effective for contract and property rights enforcement. However, it is also expensive, cases can move slowly, and juries often are persuaded to grant remarkably large amounts of damages. On the 2012 Fraser Institute Index of Economic Freedom's component index for "Legal System and Security of Property Rights", the US receives a score of 7.12 out of 10, which ranks it 33rd in the world.[681]

9. Technology Transfer

The United States does not subject foreign investors to technology transfer requirements, joint venture technology contribution requirements, or license registration requirements.

675 21 U.S.C. § 355.

676 42 U.S.C. §262(i).

677 Wendy H. Schacht & John R. Thomas, Follow-On Biologics: The Law and Intellectual Property Issues 1 (Congressional Research Service 2011).

678 42 U.S.C. §262(k)(7)(A).

679 EPA Pesticide Registration Manual, Chapter 10 (2010), http://www.epa.gov/pesticides/bluebook/chapter10.html.

680 EPA Pesticide Registration Manual, Chapter 10 (2010), http://www.epa.gov/pesticides/bluebook/chapter10.html.

681 Fraser Institute, Economic Freedom of the World 2012 Annual Report at 166 (2012).