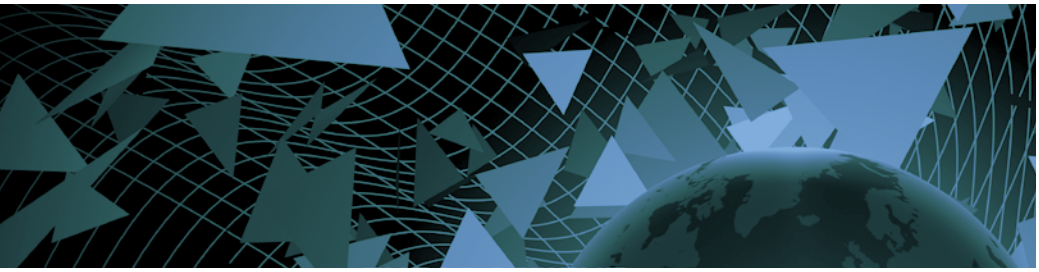
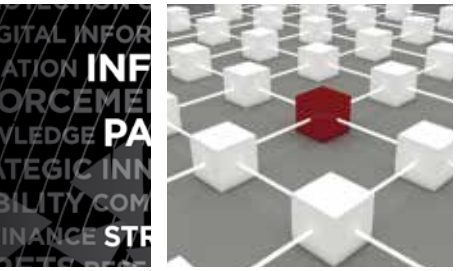
TRADE SECRETS: TOOLS FOR INNOVATION AND COLLABORATION





By Jennifer Brant and Sebastian Lohse

INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

Acknowledgements

The authors thank the following people for reviewing and providing comments on earlier drafts of this paper:

Dr. Douglas Lippoldt, Senior economist and trade policy analyst, Organisation for Economic Co-operation and Development (OECD)

Professor Cesar Parga, Chief, Competitiveness, Innovation and Technology, Organization of American States (OAS); Georgetown University Law Center

Emil Pot, General Counsel, ActoGeniX NV

Dr. Sascha Friesike, Alexander von Humboldt Institute for Internet and Society

Professor Mark F. Schultz, Senior Scholar, Center for the Protection of Intellectual Property, George Mason University School of Law & Associate Professor, Southern Illinois University School of Law

James Pooley, author of Trade Secrets (Law Journal Seminars-Press)

The views expressed in this publication are those of the authors and do not necessarily reflect those of ICC.

This publication is the third of a series of research papers in ICC's innovation and intellectual property series. The paper and more information on the project can be found at www.iccwbo.org/Innovation-and-intellectual-property.

Information on ICC's Commission on Intellectual Property can be found at www.iccwbo.org/ip-commission.

ICC thanks the following for their support of this project:

Confederação Nacional da Indústria (CNI)

CropLife International (CLI)

Dannemann Siemsen Bigler & Ipanema Moreira

Deutsche Industrievereinigung Biotechnologie (DIB)

DuPont Pioneer

General Electric

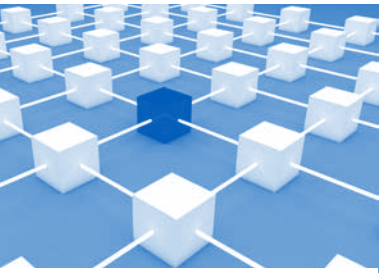
International Federation of Pharmaceutical Manufacturers & Associations (IFPMA)

INTERPAT

Shell

Unilever


MOBILITY
INNOVATION
TRADE SECRETS
PATENTS
PATENTS



Trade Secrets: Tools for Innovation and Collaboration

This paper intends to inform policymakers about the contribution of trade secrets to knowledge transfer and collaborative innovation, with emphasis on technological know-how. It also aims to inform policymakers about certain shortcomings in existing frameworks for trade secret protection, which can undermine cross-border collaboration in particular.

The first part examines the notion of trade secrets, and explains their relationship to patents, demonstrating how businesses can deploy both approaches to efficiently manage their intellectual assets. The second part of this paper looks more closely at the practical challenges of managing trade secrets in the real economy. Finally, the last section suggests actions at the firm and legislative levels to ensure that confidential business information, a key source of competitive advantage for many firms, can be successfully protected and managed

Introduction

Trade secrets include any protected business information – whether technical, financial, or strategic – that is not generally known and that provides a competitive advantage to the owner. Innovative businesses use trade secrets throughout their operations, and they value them as a way to manage their proprietary knowledge. Trade secrets and patent protection are complementary, and businesses tend to use these tools in combination in order to most effectively manage their intellectual assets.

Today's approaches to collaborative innovation require broad sharing of confidential business information. Trade secret protection can facilitate sharing among partners by enabling recovery should a third party misappropriate valuable information. Absent protection, 40 per cent of companies in the European Union (EU) report they would likely retain business information strictly internally, to avoid losing control over it (EU 2013).

From a practical point of view, existing trade secret regimes are ineffective due to low levels of legal protection, legal fragmentation across and within countries and regions, and inadequate enforcement. The resulting legal uncertainty is particularly problematic in light of today's business environment, which is characterized by globally dispersed research and development (R&D), employee mobility, and reliance on information and communication technology (ICT). A case in point is the storing and processing of digital information on external servers, which allows trade secret theft to be initiated from anywhere in the world. This, in turn, obliges companies to recover where the misappropriation occurs – often in jurisdictions that offer little or no effective protection.

Defining Trade Secrets

While its legal definition varies across jurisdictions, a trade secret can encompass any information with the following characteristics:

(i) It is not generally known or readily accessible;

(ii) It has commercial value because it is secret; and

(iii) The owner has taken reasonable steps to keep it secret.[1]

Therefore, unlike patents, the scope of trade secrets is virtually unlimited (Lemley 2008). Trade secrets extend to such diverse categories as: formulas; know-how; contract terms; software; customer lists; marketing, finance, or strategy information; and information about suppliers, competitors, and other industry participants (Chally 2004; Quinto & Singer 2012). Commercial value encompasses potential as well as actual value. Therefore, trade secret protection also applies to uncommercialized experimental work and unreleased products or strategies. Moreover it can cover combinations of elements, each of which is in the public domain. The ultimate criterion being the information's value and not its actual use, trade secrets can even protect "negative know-how", *e.g.*, erroneous research approaches or results of failed experiments (Jorda 2007).

1 Trade secret definitions are similar across jurisdictions, generally corresponding to the criteria articulated in Article 39 of TRIPS (Schultz & Lippoldt 2014), reflected in the United States' 1985 Uniform Trade Secret Act (UTSA), and set forth in the 2013 Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use, and disclosure.

According to courts and commentators, the third factor, *i.e.*, reasonable secrecy precautions on the part of the holder, is of central importance (Chally 2004). The requirement to undertake no more than "reasonable efforts" to maintain confidentiality corresponds to a key economic justification for enacting trade secret laws. In the absence of legal protection, the amount spent by owners and takers could escalate without yielding any social benefit (Risch 2007). What is "reasonable" can vary according to circumstances, especially technological developments.[2] A company that performs all its operations within a single building may adequately address misappropriation risks through basic employee agreements and visitor precautions. However, a globally networked enterprise may be expected to deploy sophisticated technologies to detect and prevent cyber-theft, entailing potentially substantial costs.

The modern definition of trade secrecy is reflected in the United States' (US) Uniform Trade Secrets Act and 1995 Restatement of Unfair Competition, as well as in the definition of "undisclosed information" provided in Article 39 of the 1995 World Trade Organization Agreement on Trade Related Aspects of Intellectual Property (TRIPS). TRIPS identifies the same three requirements, namely, secrecy, value derived from secrecy, and reasonable efforts to protect on the part of the owner. Following the adoption of TRIPS, throughout the world, the basic standards for defining a commercial secret have tended to converge on these elements.

As with the basic concept and definition of trade secrets, there is broad agreement on what actions constitute misappropriation, though the coverage in law may vary by country (Schultz & Lippoldt 2014). In situations where the information was shared under an obligation of confidence and limited use, any unauthorized disclosure or use is generally unlawful. In many jurisdictions, liability also exists for the acquisition of the information in a "manner contrary to honest commercial practices". Moreover, any use or disclosure by someone who obtains the information with knowledge of its improper acquisition is generally considered unlawful.[3]

It is important to note that, unlike patents, trade secrets are non-exclusive. For instance, it is not misappropriation to independently discover the secret information, or to reverse engineer it from a properly obtained source. Provided it was discovered through such means, the owner of a trade secret cannot prevent others from manufacturing, selling, or otherwise working the subject of the trade secret. As a result, there can be multiple holders of a similar trade secret. In contrast, a patent owner can prevent others from working his or her invention as described in the patent claims.

While there is general agreement about the nature of trade secrets and, in many jurisdictions, what sort of behaviour should be actionable as misappropriation, there is considerable variation internationally in terms of available remedies and enforcement mechanisms. As discussed later in this paper, effective enforcement is critical to trade secret owners. Without it, the legal promise of protection can be an illusion.

2 In *E.I. DuPont v. Christopher*, a well-known misappropriation case in the US, a court convicted the defendants who had taken aerial photographs of an industrial facility housing a secret process while it was under construction and thus exposed to view from above. The judges deemed the costs associated with placing a temporary cover over the site during the entire construction period as unreasonably high, while also emphasizing the morally reprehensible conduct on the part of the perpetrators. *E.I. du Pont de Nemours & Co. v. Rolfe Christopher,* 431 F.2d 1012 (5th Cir. 1970).

3 Acquisition of information in a "manner contrary to honest commercial practices" is referred to in Article 39, footnote 10, of the TRIPS Agreement. Note that certain jurisdictions, such as Indonesia, Malaysia, and the Philippines, do not recognize third-party misappropriation as a crime. *See* Schultz & Lippoldt 2014.

In today's business environment, valuable business secrets must be shared with employees, suppliers, licensees, and other partners. The law accommodates this need by treating secrecy as relative. Trade secret protection is not lost because a secret is disclosed to someone with a need to know it and who can be trusted with it (Jorda 2007). Of course, if dispersed broadly, the information can become difficult to control as a practical matter. Indeed, some argue that although trade secrets can benefit from potentially permanent protection, in reality they often lose their status at some point due to leakage, independent discovery, or reverse engineering of publicly available products.

It is this non-exclusivity that, in the view of some scholars and courts, makes trade secrets particularly fragile and possibly weaker than other intellectual property rights (IPR). However, the popularity of trade secret protection reflects how relatively easy and inexpensive it can be to apply, depending on the circumstances. In addition, it may mirror the time-sensitive value of much information; loss of secrecy matters less when the market advantage it offers has already deteriorated. For an overview on the evolution of trade secrets protection, see Box 1.

BOX 1: Evolution of trade secret protection

Trade secrets are perhaps the oldest form of intellectual property (IP) protection. As has been reported, methods for harvesting and weaving silk were protected for centuries by keeping them within a particular region of China, and after the secrets were appropriated and brought to Byzantium in the sixth century, they were closely guarded there as well. The medieval craft guilds reduced the risk of the master's sharing trade secrets with an apprentice by allowing claims against an apprentice who did not finish his committed number of years, and against a competitor trying to entice away an apprentice (Epstein 1998).

Modern trade secret laws developed in the nineteenth century from an Anglo-American jurisprudence combining theories of breach of confidence, unfair competition, unjust enrichment, and trespass (Lemley 2008). As it progressed, the doctrine drew on a series of contract and common law rules pertaining to the employment relationship. In many cases, the courts construed trade secrets as property rights (Aplin *et al.* 2012). However, by the early twentieth century, the theoretical focus shifted to protection of confidential relations and misappropriation was treated as a tort, as expressed in the US Restatement (First) of Torts §§ 757-759 (1939). In the following decades, this approach was found lacking, since it sometimes allowed for the protection of information that was in the public domain.

By the 1980s, a view of trade secrets as based in some combination of contracts and property began to prevail, as reflected both in US Supreme Court rulings and in state legislatures, the majority of which have adopted the Uniform Trade Secrets Act (UTSA) (Lemley 2008). The Restatement (Third) of Unfair Competition §§ 39-45 (1995) has been widely embraced as the modern expression of trade secret protection theory (Pooley 2013).

Sources: Aplin et al. (2012); Epstein (2008); Lemley (2008); Pooley (2013)

Relationship Between Trade Secrets and Patents

All patentable inventions begin as trade secrets (Pooley 1997), in that trade secrets can be used to protect pre-patented R&D, and both patents and trade secrets provide important incentives for innovation and investments in risky R&D ventures. However, there are important differences in the rationale and practical operation of these methods of protection. Trade secrets, unlike patents, require no registration and thus no government fees or other formalities in the majority of jurisdictions. They exist upon creation, merely by virtue of their potential commercial value and being kept secret. While trade secrets can consist of any useful information, the subject of a patent is always technical and must meet strict patentability criteria such as novelty and non-obviousness.

Patent systems provide a time-limited exclusive right in exchange for public disclosure, facilitating the dissemination of information, reducing replication of inventive efforts, and enabling inventors to build on prior work. This exclusive right may permit the patent holder to recover R&D investments and appropriate the value of his creation, at the same time enabling the public to benefit from the publication of technical information about the invention. Because patents are limited in time, the invention will ultimately enter the public domain. Trade secrets, unlike patents, are non-exclusive. In principle, trade secrets have potentially infinite duration, though in practice they often degrade over time.

Patent infringement is based on strict liability, in the sense that infringement may occur unintentionally. In contrast, in the case of trade secret misappropriation, it is generally necessary to establish that the defendant engaged in inappropriate means to obtain the information or knew it was obtained or used improperly.[4]

Some have questioned whether the protection of inventions without disclosure, in the form of trade secrecy, is good public policy. More specifically, the seemingly opposing rationales of trade secrets and patents raise the question as to whether the former may compromise the diffusion of knowledge afforded by the latter (Czapracka 2008). However, in practice the two systems co-exist reasonably well. The existence of trade secret laws has been seen to encourage technology diffusion through licensing, since the alternative may be hoarding. At a legal level, the consistency of patent and trade secret regimes was considered and acknowledged by the US Supreme Court in *Kewanee v. Bicron*.[5]

4 In certain jurisdictions, such as Singapore, depending on the circumstances, innocent third parties may be liable even if they were not aware they had received misappropriated trade secrets. *See* Schultz & Lippoldt 2014.

5 *Kewanee v. Bicron*, 416 U.S. 470 (1974).

Table 1 **Characteristics of patents and trade secrets**

	Patents	**Trade secrets**
Public disclosure	yes	no
Subject matter requirements	■ novelty ■ inventive step ■ potential industrial application	■ cannot be generally known or readily ascertainable, cannot be the employee's own skill ■ has value because it is secret ■ reasonable efforts to maintain the secret
Registration	required	not required
Scope	defined inventions	secret, useful information
Length of protection	20 years	potentially unlimited
Acquisition costs	high	low
Litigation costs	very high	variable
Enforcement	available	variable
Geographical scope of protection	patents are granted on a national or regional basis	trade secrets laws are national

In practice, trade secrets effectively complement the patent system. Given the far broader subject matter covered, trade secret laws apply to areas that patent law cannot, allowing the protection of business plans, customer lists, and so-called "negative know-how" (Lemley 2008). Trade secrets are particularly useful in protecting tacit or non-codifiable knowledge, namely information required for the implementation of a patented invention. Indeed, technology transfer frequently involves licensing of both patents and trade secrets.[6] Thus, trade secret protection enables firms to share the complementary knowledge required to implement, but also to commercialize and improve upon, patented technologies (Jorda 2007). In certain sectors, trade secrets may constitute the most valuable part of a technology transfer agreement since a patent licence alone may not enable full deployment of a proprietary technology (Jager 2002).

Other than higher cost and additional administrative requirements, the considerable delays associated with obtaining patents may render them less effective for firms in fast-moving industries, or for firms with fewer resources. In fact, in some jurisdictions, inventors may have to wait as many as eight years before patent authorities decide whether to grant protection, though patent applications are generally published after 18 months (Cummings 2008; Lemley 2008). What is more, the enforcement of patents can be very expensive. In the United States, for instance, patent litigation can cost three times more than enforcement of trade secrets, with a median of US$ 5 million per side in legal fees for large cases (AIPLA 2013).

6 So-called "hybrid licences" covering both patents and trade secrets entail certain challenges, especially given the different terms of protection of these instruments. Generally it is recommended that separate time periods be agreed for the patent licence and trade secret licence, to account for different periods of validity and avoid competition law problems.

In light of these advantages and depending on the nature of the invention, it may be resource-effective to rely on trade secrets to protect at least part of an innovation. Trade secret protection may be an especially attractive tool for technologically innovative small and medium enterprises (SMEs), which tend to have fewer resources and limited expertise and capacity for managing intellectual assets using formal IPRs. In fact, trade secrets can apply to a range of approaches used by SMEs to capture the value of their innovations, reinforcing strategies such as lead-time, product complexity, and close customer relationships. This is not to say that patents are not equally important to small businesses. In order to signal the value of an invention to potential partners and to the marketplace, an SME may need to secure patents on key aspects of its inventions – especially in technology domains where reverse engineering is relatively easy and thus exclusivity is required. An optimal IP strategy combines trade secrets and patents (Friesike 2011).

Needless to say, businesses must assess which tool – or combination of tools – is appropriate for protecting and managing a given type of knowledge in a given context. As a general rule, because patents provide an exclusive right, they are preferable for protecting products that are easily reverse engineered or imitated. In contrast, businesses tend to consider trade secrets as more effective for processes, for which patent infringement is difficult to monitor (Levin 1987; Bhattarchaya & Guriev 2006). Trade secrets are also valuable in relation to inventions that combine existing components or ideas, which may not meet obviousness and inventive step requirements for patentability. In practice, firms tend to rely on a strategic combination of patents and trade secret protection (Box 2).

BOX 2: Complementary protection through trade secrets – a case study

Trade secrets are often used by businesses to protect information related to manufacturing processes, which typically are carried out behind closed doors. Where processes are patented and thus disclosed to the public, infringement by competitors can be difficult to detect. A company may use trade secrets to protect certain know-how related to the process, patenting other aspects such as physical machinery. Trade secrets can also be used to protect innovations that do not meet patentability criteria.

A corporation registered in the US state of Illinois, C&F, manufactured meat products. Following several years of research, it had developed a commercially valuable process for making and freezing a precooked sausage for pizza toppings. The product had the characteristics of freshly cooked sausage, while being superior to other precooked sausages in terms of price, appearance, and taste. C&F filed for patents on the equipment to make the sausage, as well as on the process itself. Subsequently the company made a number of improvements to the production process, which it kept as trade secrets.

In 1985, Pizza Hut agreed to purchase a large quantity of precooked sausage from C&F. In exchange and on the basis of written confidentiality agreements, C&F disclosed the process to some of Pizza Hut's suppliers, ostensibly to ensure that backup supplies remained available to Pizza Hut. Moreover, the company leased its specialized equipment to these suppliers and invested US$ 4.5 million in a new production facility to meet Pizza Hut's needs.

Within just a few months, Pizza Hut's other suppliers had learned how to replicate C&F's results. Pizza Hut informed C&F that it would not purchase any more sausage unless it obtained significant price reductions. In 1989, it provided IBP, another supplier that offered lower prices than C&F, with the specification and formulation of the sausage toppings, transferring the relevant information in writing as well as through personal discussions with IBP employees. In addition, IBP hired a former supervisor in C&F's sausage plant as its own production superintendent, only to dismiss him five months later after it had implemented its sausage making process. By early 1991, Pizza Hut was buying its precooked sausage topping from IBP.

C&F then sued IBP and Pizza Hut for patent infringement, and also for misappropriation of trade secrets under the Illinois Trade Secrets Act. In 1998, the district court made two findings: *first*, that the patents of C&F were invalid because the inventions had been on sale more than one year prior to the filing date, and *second*, that C&F possessed valuable and enforceable trade secrets, which had indeed been misappropriated. As a consequence, it awarded the plaintiff US$ 10.9 million in damages. In 2000, the US Court of Appeals affirmed the district court's award of damages against IBP for misappropriation but reversed its award of prejudgment interest of US$ 5.1 million.

Source: C&F Packing Co. v. IBP, Inc., 224 F.3d 1296 (Fed. Cir. 2000).

The Value of Trade Secrets for Innovators

Trade secrets are often the "crown jewels" of a firm's intellectual capital, developed over many years through myriad interactions and projects (Jorda 2007). According to recent estimates, trade secrets encompass some 70 per cent of the value of companies' intellectual assets (Bird & Jain 2008; Forrester 2010; Schwarts & Weil 2010). In one survey, respondents rated proprietary technology highly as a key source of competitive advantage, and a large majority of respondents (88 per cent) cited skills and knowledge as the most important intellectual assets (IPOA 2003).

The economic rationale for trade secret protection is two-fold: *first*, it enables firms to avoid over-investing in secrecy and thus to use their resources more cost-effectively, and, *second*, it facilitates the diffusion of knowledge by creating a safe environment for firms to share information that, for whatever reason, they have not patented (Friedman *et al* 1991; Arrasvuori *et al*. 2014). In relation to this last point, trade secret protection is particularly well suited to current approaches to innovation, which emphasize incremental change and collaboration.

As empirical evidence shows, over-investment in secrecy implies not only wasted resources, but also lost opportunities for collaboration when information cannot be safely shared externally. Over-investment in secrecy may be specific, in the form of over-protection of a particular idea, or it can be general, in the sense that a company may impose too many restrictions on employees and business partners, or may over-spend on physical infrastructure to protect confidential information.

The legal protections provided under trade secret laws serve as a substitute for physical and also contractual secrecy (Chally 2008; Lemley 2008). For instance, when hiring and assigning employees, an employer can focus on candidates' skills and appropriateness for particular roles, rather than choosing people exclusively from within a trusted inner circle (Risch 2007). On the other

hand, companies' actions to prevent leakage of trade secrets sometimes appear to be at odds with employee mobility and the use by an employee of learned skills in subsequent employment (Rowe 2005). Trade secret protection laws that provide appropriate disincentives for misappropriation help to strike a balance between employee mobility and personal development, on the one hand, and the legitimate interests of companies in securing confidentiality of their proprietary information, on the other hand.

Trade secret laws also facilitate flows of knowledge by making it less risky for firms to share knowledge. Like patents, trade secrets provide a partial solution to Arrow's Information Paradox (Lemley 2008). This paradox relates to the difficulties an inventor faces if he or she needs to share a potentially valuable but secret idea in order to exploit it commercially. Without appropriate safeguards, once knowledge is exchanged between parties, there are few disincentives against using that knowledge for commercial benefit. Thus, potential partners may withhold information because they fear creating a new competitor. However, external cooperation is an increasingly important feature of firms' innovation strategies, enabling them to combine expertise and resources, and thus to accelerate technology development as well as commercialization. By providing additional security, trade secret protection enables the sharing of knowledge between parties (Arrasvuori *et al*. 2014).

The protection afforded by trade secrets matches the needs of contemporary modes of innovation. Today, innovation is increasingly characterized by a high degree of collaboration and also by emphasis on incremental progress. Adaptation of existing solutions to local environments, one form of incremental innovation, is especially relevant in developing countries. Trade secrets help to establish secure channels for exchanges of know-how, helping to build absorptive capacity, which is defined as the ability to identify, assimilate, and apply new knowledge. They also provide an alternative tool for protecting gradual advancements for which patents may not be available or financially practical (Maskus 2012). Finally, given their relative affordability, trade secrets can provide a resource-effective line of defence to SMEs in countries at all levels of development.

To summarize, trade secrets are directly implicated in the dissemination of proprietary skills and knowledge, stimulating broader disclosure and use of information. As patent protection encourages the sharing of proprietary technology, trade secret protection facilitates the sharing of proprietary know-how and expertise (Box 3). The combined deployment of trade secrets and patents provides exclusivity to the innovator, while furthering technology transfer through licensing and other transactions (Jorda 2007). Licensing agreements that include conveyances for both forms of protection are credited with stimulating the most value creation (Cummings 2008).

BOX 3: Trade secrets and technology exchange – a case study

Semiconductor chips represent the integration of communications, computer, and consumer electronics technology into one powerful computer, often comprised of many individual processors. To successfully bring a new chip to market requires technology from different sources.

Whereas in the early years of the industry, semiconductors were designed and manufactured by the same company, today more than half of logic chips are made by factories, or "foundries", that manufacture chips designed by others.

This combination of "fabless" designers and pure foundries enables each party to focus on what it does best. However, the division of labour does not mean that each side works totally independently. Rather, technical knowledge flows throughout the development process, among the chip designers, developers of tools needed for the manufacturing process, foundries, and device manufacturers.

The development of a new commercial chip requires collaboration among at least the following entities:

- The chip designer works with the developer of the general processor architecture and the corresponding customization tools. This developer licenses the design and tools to the chip designer and provides additional know-how.
- The chip designer licenses additional electronic design automation (EDA) tools and know-how from other tool developers and/or from a foundry.
- The foundry may also license customization files to the EDA tool developers. This helps to ensure that the output from the EDA tools, which are mostly software, will be compatible with the chip manufacturing equipment used by that foundry.
- The chip designer uses the EDA tools to create the circuit layouts and software, rendering the circuit layout design in a "tape out". A tape out consists of data used by the foundry's equipment to create the masks that will be used to make the final chip. Such data is proprietary to the chip designer.
- There is also close collaboration between the chip designer and those mobile device manufacturers that will integrate the chips in their devices.

Trade secret protection is of paramount importance to each of the above developers, serving as the primary form of IP protection. The general processor architecture, customization tools, EDA tools, tape out data, supporting documentation, and associated know-how are proprietary to the respective developers of each item. Ensuring that this information, which represents significant investments in R&D, is not disseminated to competitors is critical to preserving each developer's ability to remain competitive in the marketplace.

Trade secret protection is typically sought by way of confidentiality provisions in bilateral contracts. In general, contracts limit the use of the licensed tools only for the development of the recipient's designs or products, and foundries may only use tape out information to make chips for the provider of the information. Contracts may also include licensing provisions for other forms of IP rights, such as copyrights or patents, which protect the tools and other information. However, as this type of development environment essentially involves internal processes, it is difficult to identify copyright and patent infringement. Thus, trade secrets – together with the selection of trustworthy partners – represent a critical form of protection.

Sources: The Economist (2013); interview with Philip Wadsworth, Qualcomm (March 2014)

Safeguarding Trade Secrets: Challenges at the Firm and Legislative Levels

Reports indicate that companies are increasingly vulnerable to theft of confidential information, whether due to misbehaviour of current or former employees, corporate espionage, or hacking. In the US, federal cases of trade secret theft doubled between 1995 and 2004, and are expected to double again by 2017 (Almeling 2011). In a recent survey of companies in EU countries, some 20 per cent of the respondents reported having experienced at least one attempt or act of misappropriation over the past 10 years, while about 40 per cent stated that risk has increased during that period (Baker & McKenzie 2013). According to a Japanese study, more than 35 per cent of manufacturing firms have suffered some form of technology loss (ONCIX 2011). These figures may represent only the tip of the iceberg. In fact, numerous companies may have been subject to attempts to obtain their trade secrets without being aware of them, or, for reputational reasons, companies affected may be reluctant to report their losses.

A range of related factors have led to the dramatic rise in trade secret theft, namely: the globalization of supply chains; rapid advances in ICT; the growing use of external data storage and processing facilities; the increasing importance of innovation and know-how as sources of competitive advantage; and greater job mobility. Broader availability of more sophisticated technologies and access to data have facilitated the intrusion into corporate networks and the acquisition of sensitive data by employees, contractors, consultants, suppliers, and vendors.

The implications of trade secret theft for businesses include loss of competitive advantage, core business technologies, and corporate reputation as well as diminished performance and profitability. According to the National Security Agency, US companies lose some US$ 250 billion per year due to cyber-theft of trade secrets (Rogin 2012). In the UK, businesses suffer losses of as much as GB£ 21 billion per year due to IP theft and espionage (Detica & Cabinet Office 2011).

Apart from theft, companies face misappropriation risks when providing authorities with confidential business information in the context of procedures to secure market access (Arrasvuori *et al.* 2014).[7] If information is not appropriately stored and managed by government officials, or is proactively made public by them, trade secrets can become public knowledge, losing their value. From a firm's perspective, it is critical that any such information remains confidential. Government requests should be narrowly tailored and, to the extent possible, exclude trade secret information.

Firm-level challenges

Trade secret cases generally present themselves in three basic sets of circumstances: competitive intelligence, business transactions, and departing employees (Almeling 2009). Recent advancements in ICT can enhance the risks derived from these situations.

7 For certain product categories, Article 39.3 of the TRIPS Agreement mandates the protection of confidential data that has been submitted to authorities in order to obtain marketing approval.

ICT developments

Developments in ICT have tremendously facilitated trade secret misappropriation because, today, most valuable data exists and flows in digital form. In addition, thanks to the ever-rising sophistication of mobile devices, information has become ubiquitously accessible, creating multiple vulnerabilities. In particular, corporations are increasingly storing and processing confidential information in the cloud, which can create additional risks (Box 4). It should be noted that not only persons with legitimate access but also hackers pose threats to digital trade secret information (Almeling 2012).

What is more, the rise of social media, such as Facebook, LinkedIn, and Twitter, together with a different perception of secrecy in particular among the younger generation, has created new cultural challenges for the protection of trade secrets (Arrasvuori *et al.* 2014). In this context, the requirement that the information not be "generally known" poses particular issues. For instance, a list of customers may lose its quality as a trade secret when employees communicate with them through one of the aforementioned networking sites, using their readily accessible contact lists (Warren & Pedowitz 2011).

BOX 4: Practical challenge at the firm level – trade secrets and cloud computing

Companies face myriad ICT-related issues when protecting their trade secrets. One challenge involves cloud computing, a computer networking model that provides users with on-demand access to shared data processing and storage capacities. Because of its considerable benefits, namely higher efficiency, lower costs, and greater consumer convenience, cloud computing is expected to continue its spectacular rise in use over the next years. Relinquishing control over confidential business information to the cloud service provider, however, can entail data security issues. Other than technical failure such as data outages, the main risk arises from inappropriate access by third parties.

While cloud providers claim to have the capabilities to secure highly confidential or sensitive data, instances of data theft, cases of misappropriation and inadvertent disclosure of confidential corporate information have been reported. These may result from actions by employees or former employees with authorized access, or from hacking, data mining, or corporate espionage. The ubiquitous character of public cloud systems and the necessary data access points make cloud systems particularly vulnerable.

Given such risks, users of cloud services should carefully consider the nature of information stored in this fashion. They should negotiate arrangements that match the sensitivity and vulnerability of given sets of information with the appropriate level of controls and liability allocation. At the most secure end of the spectrum, for example, completely private or securely partitioned clouds can be used. The increasing popularity, competitiveness, and sophistication of these services mean that, in most cases, an appropriate level of security can be negotiated.

Source: Savitz (2012)

Business transactions

In globalized supply chains, businesses resort to three different forms of knowledge-based sourcing transactions: captive sourcing; third-party sourcing; and joint-venture sourcing (CREATe 2012). While captive sourcing, that is, the creation or acquisition of their own operational facilities, allows companies to keep a maximum of control over their intellectual assets, it involves long implementation times and high investments. Even captive sourcing presents security risks, for example, when competitors hire away employees engaged in the building of the corporation's offshore structures. Third-party sourcing (*i.e.*, the use of external suppliers) offers rapid implementation and low costs, as well as greater flexibility in terms of production capacity. However, it can reduce the company's control over operations, in particular over confidential information.

In a joint venture, the intermediary form of sourcing, foreign companies and local entities engage in partnerships, thereby reducing start-up costs and sharing risks. Nevertheless, joint ventures entail more complicated structural and operational issues, especially as regards the regulatory framework in the offshore jurisdiction. A case in point is Chinese legislation authorizing partners to develop and claim ownership over derivative works based on licensed technology (CREATe 2012). Also, the Brazilian Patent and Trademark Office (INPI) reviews technology transfer contracts, generally prohibiting confidentiality obligations that exceed five years, as well as obligations to return technical information when a contract expires (WIPO 2013). This results in reduced protection for confidential information licensed under such agreements.

Employee mobility

Greater job mobility, a global trend affecting trade secret protection, naturally increases the risk that employees will use their former employer's trade secrets in subsequent employment (Yang & Jiang 2007). In 2008, in the sample used by one study, some 60 per cent of those accused of misappropriating confidential business information in the United States were current or former employees (Almeling 2010). Non-compete agreements can be used, depending on the jurisdiction, to help control the risk of undetectable misappropriation by former employees. However, in litigation, courts sometimes refuse to recognize agreements that appear excessive in subject matter or geographical coverage. Moreover, the laws of some countries prohibit restrictions on employee movement and their use of information learned on the job (Pooley 2013). Such variation in regulation among countries can complicate management of globalized, distributed R&D. The most commonly used controls consist of well-drafted employee nondisclosure and invention assignment agreements, coupled with careful post-separation monitoring of competitive activity.

It is essential that firms also pay close attention to trade secret issues when defining and managing other relationships, such as collaborations, joint ventures, technical assistance, and licensing, particularly hybrid patent/trade secret licences. Well-crafted agreements that anticipate potential problems such as ownership and post-relationship rights and limitations can help all involved to avoid misunderstandings and litigation.

Legal challenges

A great deal of variation exists among the trade secret protection regimes of different jurisdictions, and differences exist even within countries and economically integrated areas such as the EU. Rules on trade secrets arise from a variety of legal sources, providing different degrees of protection

and creating confusion (Schultz & Lippoldt 2014). In some legal systems, such as those of China, Germany, Poland, and Japan, general laws on unfair competition offer protection of trade secrets. In France, both the criminal code and the labour code contain provisions on trade secrets (Czapracka 2008). According to a recent study, legal protection of confidential information in World Trade Organization (WTO) member states derives from more than 25 different fields of law (WTO 2013).

In certain common law countries, such as India, there is a focus on breach of duty rather than misappropriation. In such places, trade secret protection may be limited to cases covered by contract and employment relationships, making misappropriation claims more difficult, for instance, when asserted against a subcontractor or other actor with whom the owner of the trade secret has no contractual relationship (Schultz & Lippoldt 2014).

In jurisdictions where there is no specific trade secret legislation, and enforcement is based on contracts with suppliers and partners, or employee relationships, it can be difficult to prosecute a misappropriator who has no direct contractual relationship with the trade secret owner, such as a subcontractor working for a supplier.[8] In such cases, the owner may have to depend on the cooperation of the contractor to pursue the problem legally. The owner should pay careful attention to contract drafting, in addition to limiting the sharing of trade secrets to only those with whom the owner has a direct relationship. Confidentiality undertakings by subcontractors, to the direct benefit of the owner, may also be sought.

The most important weaknesses in legal protection regimes are:

- **Inadequate civil or criminal remedies to deter infringers.** Insufficient remedies very often fail to deter potential infringers. For instance, Canada's criminal law neither addresses trade secrets explicitly nor offers viable alternative means to prosecute their misappropriation.[9] Moreover, while many countries provide civil remedies at the national level so that victims of trade secret theft can more efficiently recover damages and stop misappropriation, others, such as the US, offer no federal civil remedies.
- **Inadequate injunctive relief, or unavailable *ex parte* orders.** Preliminary and permanent injunctions are critical tools for reducing and stopping the damage from trade secret misappropriation. In addition, *ex parte* seizures are often needed to preserve evidence of misappropriation, particularly if it has been stored electronically and the trail could be easily erased.
- **Failure to protect confidentiality of trade secrets during legal proceedings.** Once a trade secret has been revealed, its value is destroyed. This can happen during open legal proceedings, exposing the secret to competitors and effectively compromising trade secret protection provided under statutes. Because trade secrets must be revealed to the court in order to seek relief, a trade secret owner may have to weigh the possible damage from further exposure of the information against the benefits of recovery. This can deter an owner from seeking relief.

8 As part of a debugging project, an employee of an Indian company, Geometric Software Solutions Ltd., had been given access to software source code owned by SolidWorks, a US-based client of that firm. After leaving Geometric Software Solutions, the employee was caught trying to sell the software code, worth US$ 50 million, to SolidWorks' competitors for some US$ 200,000. As Indian law does not recognize the misappropriation of trade secrets, it was not possible to sue the individual. Since the source code belonged to SolidWorks, the ex-employee technically had not stolen from his employer (CREATe 2012).

9 Section 18 of the Security of Information Act (SOIA), which criminalises the release of trade secrets "to the detriment of Canada's economic interests, international relations or national defence or national security", does not appear to have been relied upon by businesses to address trade secret misappropriation not related to national security.

- **Inadequate enforcement.** Even in countries where legislation provides for remedies, there may be no guarantee of effective enforcement, which largely depends on capacity and political will (Peterson 2008). In Mexico, for instance, a reported 97 per cent of industrial espionage cases are not prosecuted and, of the cases that are brought to court, only 56 per cent result in damages or fines (GIPC 2013).
- **No mechanisms for procedural cooperation.** In general, legislators fail to adopt provisions that govern the interplay between relevant government agencies in case of trade secret misappropriation. This complicates trade secret protection and enforcement within jurisdictions. At the same time, a lack of international mutual legal assistance complicates protection and enforcement across borders.

In addition to weak protection, another problem that trade secret owners face is legal fragmentation. Even in countries with relatively well-developed regimes for protecting trade secrets, fragmentation may be an issue. For instance, in the United States, notwithstanding adoption of the Uniform Trade Secret Act (UTSA) in 1985, trade secret laws are not fully unified at the state level (Almeling 2009). With trade secret theft today increasingly crossing state and national lines, companies have expressed frustration with the inability of state courts in the US to respond effectively to trade secrets misappropriation, given that they lack the power of nationwide service of process and discovery implementation.

Moreover, the lack of substantive and procedural uniformity may entail certain costs for courts and litigants, which must take account of the inter-state differences. For instance, in the Pizza Hut case study (Box 1), the plaintiff company, C&F, sued Pizza Hut under the Illinois Trade Secrets Act, because C&F was an Illinois corporation and Pizza Hut operated in Illinois.[10] However, the district court dismissed that trade secret claim because, the court found, the claim should have been filed under the Kansas Uniform Trade Secret Act, and the Kansas law had a shorter statute of limitations than Illinois (three years instead of five). While the Federal Circuit vacated that decision and reinstated the Illinois trade secrets claim, the process cost C&F additional time and money.[11]

The differences in legal trade secret protection are more pronounced within the EU. Sweden is one country that has enacted a stand-alone law on trade secrets (Box 5), though other countries, such as Italy and Portugal, have specific provisions in their IP legislation providing for trade secret protection. Most EU members, however, afford protection through various provisions of civil and criminal legislation, including unfair competition law, contract law, common law, and codes of industrial property. This legal division entails costs and difficulties of enforcement across borders, and creates considerable uncertainty as to where to locate R&D centres, where to engage in partnerships, and how to allocate responsibilities among employees located in different jurisdictions, each with their own rules governing employees' use of confidential business information in subsequent employment. Legal fragmentation adversely affects the appropriation and dissemination of information, know-how, and technology throughout the EU (Baker & McKenzie 2013).

10 *C&F Packing Co., Inc., v. IBP, Inc.*, 224 F.3d 1296, 1300 (Fed. Cir. 2000).

11 *Id.* at 1306.

BOX 5: Elements of trade secret protection – analysis of Sweden's trade secrets regime

Sweden is one of the few countries worldwide to have adopted a comprehensive statute on the protection of confidential business information. The 1990 Trade Secrets Act offers an explicit definition of trade secrets, criminalizes trade secret espionage, and comprises provisions on civil liability. Though certain improvements are needed, the Act could provide a basic model for trade secret protection in Europe.

Definition. Under the Act, a trade secret is defined based on three elements: (i) it must concern business or operating conditions of a business; (ii) it must be confidential; and (iii) disclosure of the information must harm the competitive position of the owner. The definition does not specify what efforts may be required to keep the information secret.

Cause of action. Anyone who wilfully and without authorization obtains access to trade secrets can be convicted of trade espionage, with penalties including imprisonment of up to six years. Unauthorized access is considered to cause loss of control over the information and a risk of damage to the owner. Actual exploitation of the trade secrets on the part of the owner is not a prerequisite for finding a criminal offence.

Deterrent damages. Damages differ according to whether the infringer is a business partner, an employee, a former employee, or a third party. Anyone committing a criminal offence under the Act may be liable for the damage caused by his or her action, as well as for any damages resulting from the subsequent unauthorized use or disclosure of the trade secret. The Act also contains provisions for recovery of damages for breach of confidentiality obligations in a business relationship and employment contracts. More particularly, it provides for post-employment damages in the presence of "extraordinary reasons". According to Swedish case law, these include an employee collecting information during employment with intention to start a competing business after his or her departure. While courts have reported difficulties in quantifying adequately the damage caused, compensation is generally set at a level such that unauthorized use of a trade secret is not financially more lucrative than obtaining the information in question legally.

Injunctive relief. The Act provides for injunctive relief. In particular, interim injunctions are available if the plaintiff can demonstrate that the trade secret has been subject to unauthorized use, access, or disclosure, and that it is reasonable to assume that such acts will continue thus undermining the trade secret's value.

Remaining challenges. While the Swedish Act on the Protection of Trade Secrets is generally considered as comprehensive and effective, commentators have identified a number of important shortcomings. First, the criminal provisions of the statute do not apply to a party that originally had legal access to the information at issue, such as an employee who discloses trade secrets. Second, although it is possible to obtain orders for ***ex parte* seizures** under the Act, the latter fails to fully implement the EU Enforcement Directive to allow parties to effectuate an emergency search of the alleged infringer's premises to secure evidence. Third, the statute does not contain any particular rules on trade secret **protection during litigation**, and the Constitution

provides that all information relied upon in court litigation should be available to the general public unless there are statutory rules to the contrary.

Sources: Levin et al. (2010); Hogan Lovells (2012); Schultz & Lippoldt (2014)

Having already harmonized some aspects of IP law (*e.g.*, trademarks, industrial designs, standards for software, biotechnical inventions, and databases), the EU has begun to undertake similar efforts in the area of trade secrets. In November 2013, recognizing the considerable economic harm brought about by the theft and misuse of business confidential information, the EU Commission published a Draft Directive that proposes a common definition of trade secrets, as well as a range of instruments through which victims of trade secret misappropriation can obtain redress.[12] The proposal intends to facilitate the necessary actions in national courts, the removal of trade secret-infringing products from the market, and the grant of damages for victims of trade secret misappropriation (EU 2013).

The business community has welcomed the prospect of harmonized legislation on trade secrets in the EU, which could bolster innovation and economic growth by removing existing obstacles to the internal market for know-how, in particular transaction costs and risks associated with an inadequate legal framework (Baker & McKenzie 2013). Through improved trade secret protection, the Commission hopes to attract firms to develop, exchange, and share innovative knowledge within the EU, thus reinforcing regional competitive advantages (EU 2013).

Internationally, trade secret protection remains extremely fragmented, in part because the TRIPS Agreement does not detail implementation of the trade secret obligations it imposes. Such fragmentation is out of step with today's globalized business environment. This is particularly true as regards data management. Increasingly, firms store and process information with third parties. They no longer retain confidential information in one physical location, such as headquarters or a manufacturing facility, where protective measures can effectively prevent leakage. Today, trade secret theft can be initiated from anywhere in the world, and recovery is generally based on the laws where the misappropriation takes place. Moreover, given the ease of copying and transporting information in digital form, a person can download information then easily carry it across borders, escaping prosecution or, at the very least, forcing the trade secret owner to duplicate efforts already initiated elsewhere. In short, variations in trade secret laws and remedies from country to country, or across regions within a country or economically integrated area, make it very difficult to stop and prosecute trade secret misappropriation.

Moreover, where legal protection of confidential information is weak, trade secret theft may become pervasive – even to the point that it constitutes a part of corporate strategies in certain IP-intensive industries. Given the interconnectedness of the global economy, the creation of a sound foundation for trade secret protection and enforcement will require national, plurilateral, and multilateral efforts with the participation of a maximum number of countries.

12 The Draft Directive (see footnote 1) is part of the flagship initiative "Innovation Union", one of the pillars of the "EU 2020 strategy", under which the European Commission aims to create a more innovation-friendly environment. In May 2014, the Council of the EU agreed on a general approach for establishing a new legal framework for the protection of trade secrets. That document articulates the Council's position on the proposed Directive, paving the way for negotiations with the European Parliament with a view to reaching an agreement at first reading.

Plausible Solutions

This paper describes the value of trade secrets to innovative firms of all sizes and the role of trade secret protection in facilitating knowledge flows. At the same time, it identifies several factors that complicate the protection and management of trade secrets in today's business environment. Many of the factors relate to the business environment itself, which is characterized by networked R&D and open innovation, globally dispersed teams of employees, increased employee mobility, digital storage of data, and the growing value of know-how as a source of competitive advantage – and thus a target for corporate theft.

Other risk factors derive from inadequate legal frameworks for trade secret protection, which make it difficult for trade secret owners to recover in the event of misappropriation. Legal fragmentation across countries, and even within countries and economically integrated areas, compounds this difficulty and further compromises collaboration and the sharing of know-how with external partners.

Ensuring that confidential business information is adequately protected from misappropriation requires **action at the firm level**, first and foremost. Companies must develop a trade secret policy and integrate it into the company code of conduct. They should put in place appropriate physical and digital security measures to protect trade secrets, routinely mark relevant information as "confidential", and consider housing the most sensitive information in jurisdictions with robust trade secret regimes. It is critical that firms educate employees about their obligations of confidentiality, during the term of employment and at departure, and such obligations should be explicitly listed in employee contracts. Firms should limit business information provided to third parties, and should require external partners such as suppliers to restrict, monitor, and record access by employees and subcontractors to their confidential information. With regard to employees and external partners alike, it is important that firms take appropriate action after the business relationship has ended.

In addition to its own actions, a firm's ability to retain control over its confidential data, and to recover without exposing itself to further risk, will depend in large part on the legal frameworks in relevant jurisdictions.

The fragmentation of trade secret protection frameworks creates major challenges, given the globalized nature of doing business and the prevalence of open innovation. **Convergence of trade secret legislation across jurisdictions** could provide legal certainty and enable owners of trade secrets to more effectively address misappropriation, wherever initiated. This in turn could enhance knowledge flows and cross-border investments in R&D. Policymakers should address trade secrets systematically in free trade agreements, such as the Trans-Pacific Partnership Agreement and the Trans-Atlantic Trade and Investment Partnership Agreement. In particular, policymakers should work to establish common rules to address cross-border misappropriation cases.

Action at the domestic level will be an important complement to such international efforts. Policymakers should enact **clear provisions on trade secret protection**, whether in a stand-alone law or as part of legislation providing for the protection of other types of IPRs. Trade secret laws should include a clear definition of trade secrets based at least on Article 39.2 of the TRIPS Agreement. They should define and criminalize conduct amounting to a serious trade secret violation, including third party misappropriation, while providing for both individual and corporate liability. Trade secret protection frameworks should contain a comprehensive set of interim and final remedies. They should include effective tools to preserve, facilitate, and secure the gathering

of evidence, including disclosure orders and *ex parte* search orders for premises and IT systems. Criminal and civil remedies, including damages, must be structured so as to constitute a deterrent to trade secret misappropriation. Policymakers should also ensure confidentiality of trade secrets during legal and administrative proceedings, so that recovery does not lead to further disclosure and losses for the trade secret owner. Finally, trade secret and related laws should adopt a balanced approach to employee mobility, providing for the protection of confidential information without unduly restricting individuals' opportunities for professional development.

Policymakers and industry groups may consider providing **training for SMEs**, to guide them in using trade secrets as part of their intellectual asset management strategies. Compared to larger firms, SMEs have relatively lower levels of experience with and fewer resources to dedicate to IP management. Innovative SMEs are likely to benefit from training on the appropriate actions they must take to protect confidential business information, in order to be able to enforce their rights before the courts in the event of misappropriation. They could also benefit from insights into how to institute effective processes for managing confidential information internally and vis-à-vis partners.

References

Almeling DS (2009) Four Reasons to Enact a Federal Trade Secrets Act. *Fordham Intellectual Property, Media & Entertainment Law Journal* **19,** 769-798.

Almeling DS (2012) Seven Reasons Why Trade Secrets Are Increasingly Important. *Berkeley Technology Law Journal* **27,** 1091-1117.

Almeling DS, Snyder DW, Sapoznikow M, McCollum WE, Weader J (2011) A Statistical Analysis of Trade Secret Litigation in State Courts. *Gonzaga Law Review* **46,** 57-101.

American Intellectual Property Law Association [AIPLA] (2013) *Report of Economic Survey.*

Aplin T, Bently L, Johnson P, Malynicz S (2012) *Gurry on Breach of Confidence: the Protection of Confidential Information*. 2nd ed. Oxford University Press.

Arrasvuori J, Liang, L, Kuusisto, J (2014) *Management of Confidential Business Information: Results of the International Telephone Survey 2014.*

Baker & McKenzie (2013) *Study on Trade Secrets and Confidential Business Information in the Internal Market.* Prepared for the European Commission.

Bhattacharya S, Guriev S (2006) Patents vs. Trade Secrets: Knowledge Licensing and Spillover. *Journal of the European Economic Association* **4,** 1112-1147.

Bird RC, Jain SC (2008) *The Global Challenge of Intellectual Property Rights.* Elgar Publishing, Cheltenham.

Chally J (2004) The Law of Trade Secrets: Toward a more efficient approach. *Vanderbilt Law Review* **57,** 1269-1311**.**

CREATe (2012) *Trade Secret Theft – Managing the growing threat in supply chains.* White Paper. CREATe, Washington.

Cummings SW (2008) The Role of Trade Secrets in Today's Nanotechnology Patent Environment. *Nanotechnology Law & Business* **5,** 41-51.

Czapracka KA (2008) Antitrust and Trade Secrets: The US and the EU Approach. *Computer & High Technology Law Journal* **42,** 207-273.

De Carvalho NP (2010) *The TRIPS Regime of Patent Rights*. 3rd ed. Kluwer Law International, Alphen aan den Rijn.

Detica, Government Office (2011) *The Cost of Cybercrime – Full Report.* London.

Dobrusin EM, Krasnow RA (2012) *Intellectual Property Culture: Strategies to Foster Successful Patent and Trade Secret Practices in Everyday Business*. Oxford University Press, New York.

Epstein SR (1998) Craft Guilds, Apprenticeship, and Technological Change in Preindustrial Europe. *The Journal of Economic History* **58,** 684-713.

EU (2013) Impact Assessment accompanying the document proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. Commission Staff Working Document. European Commission, Brussels.

Forrester Consulting (2010) *The Value Of Corporate Secrets: How Compliance And Collaboration Affect Enterprise Perceptions Of Risk.* Forrester Consulting Thought Leadership Paper.

Friedman DD, Landes WM, Posner RA (1991) Some Economics of Trade Secret Law. *Journal of Economic Perspectives* **5,** 61-72.

Friesike S (2011) *Profiting from Innovation by Managing Intellectual Property*. PhD thesis. University of St. Gallen.

Global Intellectual Property Center [GIPC] (2013) *Measuring Momentum – The GIPC International IP Index.*

Gong J, Png IPL (2012) *Trade Secrets Laws and Inventory Efficiency: Empirical Evidence from U.S. Manufacturing.*

Hogan Lovells (2012) *Report on Trade Secrets for the European Commission.* London.

Intellectual Property Owners Association [IPOA] (2003) *Survey on Strategic Management of Intellectual Property*.

Jager M (2002) The Critical Role of Trade Secret Law in Protecting Intellectual Property Assets. In: Goldschneider R (ed) *The LESI Guide to Licensing Best Practices.* Wiley, Hoboken, New Jersey.

Jorda KF (2007) Trade Secrets and Trade-Secret Licensing. In: Krattiger A, Mahoney RT, Nelsen L (eds) *Intellectual Property Management in Health and Agricultural Innovation: A Handbook of Best Practices.* MIHR, Oxford.

Lemley MA (2008) The Surprising Virtues of Treating Trade Secrets as IP Rights, *Stanford Law Review* **61**, 311-354.

Levin M, Penaloza Isacson S, Sandgren E, Ulfsdotter S, Wainikka C (2010) *Protection of Trade Secrets Through IP and Unfair Competition Law.* AIPPI Report Q215, Sweden.

Levin RC, Klevorick AK, Nelson RR, Winter SG (1987) *Appropriating the Returns from Industrial Research and Development.* Brooking Papers on Economic Activity 3/1987. 783-831.

Maskus KE (2012) *Private Rights and Public Problems: The Global Economics of Intellectual Property in the 21st Century.* Peterson Institute Press, Washington DC.

ONCIX (2011) *Foreign Spies Stealing US Economic Secrets in Cyberspace. Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011.* Office of the National Counterintelligence Executive, Washington DC.

Peterson EA (2012) Global Strategic Collaboration: Trade Secrets and Firm Value. *Journal of Management and Sustainability* **2,** 178-186.

Pooley J (1997) The Top Ten Issues in Trade Secret Law. *Temple Law Review* **70,** 1181-1190.

Pooley J (1997-2013) *Trade Secrets*. Updated Treatise. Law Journal Seminars-Press, New York.

Quinto DW, Singer SH (2012) *Trade Secrets: Law and Practice.* 2nd edition. Oxford University Press.

Risch M (2007) Why Do We Have Trade Secrets? *Marquette Intellectual Property Law Review* **11,** 1-76.

Risch M (2010) Trade Secret Law and Information Development Incentives. In: Dreyfuss RC, Strandburg KJ (eds) *The Law and Theory of Trade Secrecy. A Handbook of Contemporary Research*. Edward Elgar, Celtenham.

Rowe EA (2005) When Trade Secrets Become Shackles: Fairness and the Inevitable Disclosure Doctrine. *Tulane Journal of Technology and Intellectual Property* ***7,*** 167-226.

Savitz E (2012) Is It Safe To Store Your Trade Secrets In the Cloud? *Forbes Magazine*, February 22, 2012.

Schiller AA (1930) Trade Secrets and the Roman Law: the *Actio Servi Corrupti*. *Columbia Law Review* **30,** 837-845.

Schultz MF, Lippoldt DC (2014) *Approaches to Protection of Undisclosed Information (Trade Secrets).* Trade Policy Paper 162. OECD, Paris.

Schwarts RS, Weil MD (2010) *United States Law on Restrictive Covenants and Trade Secrets. American Law Institute*. American Bar Association Continuing Legal Education ST001, 2291.

The Economist (July 27, 2013) *A fab success. The smartphone boom has been a boon for a pioneer in semiconductors.*

Warren M, Pedowitz A (2011-2012) Social Media, Trade Secrets, Duties of Loyalty, Restrictive Covenants and Yes, the Sky is Falling. *Hofstra Labor & Employment Law Journal* **29,** 99-113.

Watson A (1996*) Trade Secrets and Roman Law: The Myth Exploded*. Tulane European and Civil Law Forum **11,** 19-29.

WIPO (2013) *Survey on Technology Transfer Agreements and Antitrust*. Geneva.

Yang Q, Jiang C (2007) Location advantages and subsidiaries' R&D activities in emerging economies: exploring the effect of employee mobility. *Asia Pacific Journal of Management* **24,** 341-358.

THE INTERNATIONAL CHAMBER OF COMMERCE (ICC)

ICC is the world business organization, a representative body that speaks with authority on behalf of enterprises from all sectors in every part of the world.

The fundamental mission of ICC is to promote open international trade and investment and help business meet the challenges and opportunities of globalization. Its conviction that trade is a powerful force for peace and prosperity dates from the organization's origins early in the 20th century. The small group of far-sighted business leaders who founded ICC called themselves "the merchants of peace".

ICC has three main activities: rule setting, dispute resolution, and policy advocacy. Because its member companies and associations are themselves engaged in international business, ICC has unrivalled authority in making rules that govern the conduct of business across borders. Although these rules are voluntary, they are observed in countless thousands of transactions every day and have become part of the fabric of international trade.

ICC also provides essential services, foremost among them the ICC International Court of Arbitration, the world's leading arbitral institution. Another service is the World Chambers Federation, ICC's worldwide network of chambers of commerce, fostering interaction and exchange of chamber best practice. ICC also offers specialized training and seminars and is an industry-leading publisher of practical and educational reference tools for international business, banking and arbitration.

Business leaders and experts drawn from the ICC membership establish the business stance on broad issues of trade and investment policy as well as on relevant technical subjects. These include anti-corruption, banking, the digital economy, marketing ethics, environment and energy, competition policy and intellectual property, among others.

ICC works closely with the United Nations, the World Trade Organization and intergovernmental forums including the G20.

ICC was founded in 1919. Today its global network comprises over 6 million companies, chambers of commerce and business associations in more than 130 countries. National committees work with ICC members in their countries to address their concerns and convey to their governments the business views formulated by ICC.

INTERNATIONAL CHAMBER OF COMMERCE

The world business organization

33-43 avenue du Président Wilson, 75116 Paris, France
T +33 (0)1 49 53 28 28 F +33 (0)1 49 53 28 59
E icc@iccwbo.org www.iccwbo.org

Publication number: 450/1081-3
ISBN: 978-92-842-0287-4