PROTECTING TRADE SECRETS—RECENT EU AND US REFORMS

GUIDANCE FOR BUSINESSES

RECOMMENDATIONS FOR POLICY MAKERS WORLDWIDE

INTERNATIONAL CHAMBER OF COMMERCE

Contents

Acknowledgements

Task force co-Chairs

- Stefan Dittmer, Dentons, Germany *(Task Force Co-Chair)*
- James Pooley, United States *(Task Force Co-Chair)*

Chapter coordinators and lead drafters

- Russell Beck, Beck Reed Riden, United States
- Edward Blocker, Koninklijke Philips, United States
- Stephen Chow, Hsuanyeh Law Group, United States
- Patrick Coyne, Finnegan, United States
- Victoria Cundiff, Paul Hastings, United States
- Sara de Roman Pérez, Santiago Mediano Abogados, Spain
- Elio De Tullio, De Tullio & Partners, Italy
- Martina Eberle, BASF, Germany
- Cécile Foucher, Orange, France
- Andrea Garcés, Ventura Garcés & López-Ibor, Spain
- Maximilienne Giannelli, Finnegan, United States
- Reg Goeke, Mayer Brown, United States
- R. Mark Halligan, FisherBroyles, United States
- Thomas Lindqvist, Hammarskiöld & Co, Sweden
- Robert Milligan, Seyfarth Shaw, United States
- David L. Pardue, Owen, Gleaton, Egan, Jones & Sweeney, United States
- Dean Pelletier, Pelletier Law, United States
- William Smith, Bird & Bird, United Kingdom
- Peter Toren, Toren Law, United States
- Mirko Vianello, BASF, Germany
- Xinyan Wang, Luye Pharma, China
- Bettina Wanner, Bayer, Germany
- Robert Williams, Bird & Bird, United Kingdom
- Lori Zahalka, Mayer Brown, United States

Editorial team—ICC

- Angèle Beauvois
- José Godinho
- Daphne Yong-d'Hervé

Given the growing importance of trade secret protection for businesses, and in light of the pioneering legislation on trade secrets in the EU and the US, ICC has developed this report with three aims:

- Help businesses understand what measures they have to take to benefit from the protection afforded by the EU Trade Secrets Directive and the US Defend Trade Secrets Act;
- Provide more general guidance to businesses on internal practices for assessing risk, and for identifying and managing information that they wish to protect as trade secrets;
- Make recommendations to policy makers around the world considering establishing or reforming frameworks for the protection of trade secrets, based on lessons drawn from the experiences of the EU and US trade secret laws.

The following chapters address the legal status of trade secrets and specific exceptions, the identification and management of trade secrets, enforcement, available civil and criminal remedies, as well as the scope of territorial jurisdiction.

The final chapter concludes with recommendations for policy makers in all countries considering introducing or reforming trade secrets legislation drawn from the analysis of the EU and US legislation.

I. Introduction

Information and knowledge increasingly form the most valuable assets of a company. As part of these intellectual assets, confidential business information—which may include trade secrets—is of growing importance, especially in light of the globalisation of trade and interconnected supply chains.

Easier transmission of information due to digitisation and ICT has significantly increased the challenge of controlling unauthorised distribution of confidential information (i.e. information that should be kept secret). The ubiquity of devices and appliances which can be used to access information on the Internet makes this challenge all the more formidable. The need for appropriate legal frameworks to help companies to protect their valuable confidential information in this new environment is therefore recognised by both businesses and governments.

Trade secret protection, however, remains weak in many countries, due partly to the lack of specific protective legislation and partly to the lack of awareness by the judiciary and other administrative bodies. The laws in place provide for trade secret protection mainly under unfair competition law. Many of these laws expressly address the risks of leaks by employees but not by suppliers, although a significant percentage of trade secret cases result from misappropriation by suppliers and other business partners. With regard to the protection of trade secrets against abuse by employees, there are great differences in national legislations and in the employers' and authorities' powers to act in a suspected case. Violation of a confidentiality undertaking can also be treated as a breach of contract. In limited cases, such as theft or business espionage, misappropriation of trade secrets can be a criminal offence.

In 2016, important steps towards stronger protection of trade secrets were made in the EU and the US. The EU adopted the Directive on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) against their Unlawful Acquisition, Use and Disclosure (Trade Secrets Directive)[1] in June 2016, with the aim of harmonising trade secret legislation across the EU.[2] As EU Directives do not have direct effect in EU member states, each country has to enact national legislation to implement the Directive's provisions. This will result in some differences between national trade secret laws across the EU, especially because the Directive allows for different options for implementation on certain matters.

Another step forward towards broader trade secret protection is the US Defend Trade Secrets Act (DTSA) of May 2016, which creates a national standard for trade secret claims, introduces an *ex parte* seizure order procedure, and protects information provided in confidence by whistle-blowers to government or court officials.[3]

That the United States and the EU introduced sweeping new legislation on trade secrets at virtually the same time is not mere coincidence. Rather, it reflects a significant shift of business attention towards data as primary assets in an information economy. At the same time, the ever-increasing pace of R&D has led companies to pursue options of protection alternative

1 EU Directive 2016/943 of 8 June 2016, eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943 .

2 For an overview and comparison of the legal systems for the protection of trade secrets in each EU member state (prior to the implementation of the Directive), see the EUIPO report The Baseline of Trade Secrets Litigation in the EU (2018), https://euipo.europa.eu/ohimportal/fr/web/observatory/observatory-publications.

3 See https://www.congress.gov/114/plaws/publ153/PLAW-114publ153.pdf .

or complementary to patents. While the headlines speak mostly to threats from external hacking, businesses have come to realise that, in a world where valuable information must be shared, internal relationships with employees and external relationships with partners and supply chains call for special measures. For the same reasons, governments have recognised that efficient and effective sharing of commercial secrets requires robust legal frameworks to enforce undertakings of confidentiality.

While improved rules are essential, they will not solve the problem of global trade secret abuse alone. Businesses need to carry out realistic risk assessments to determine the necessary level of information security to protect trade secrets. They also need to set up adequate information security policies, measures and training programs to effectively secure their intellectual property against the growing risks of trade secret misappropriation.

II. Legal status of trade secrets

1. What is a trade secret?

A trade secret is a piece of information treated as confidential by an enterprise because its particular features combined with limited access provide a competitive advantage. Such a secret piece of information can be durable or ephemeral, so long as it helps enterprises to perform better, faster or at lower cost.

A trade secret may be almost any information that has economic value and provides the holder of the secret with an advantage over competitors by virtue of its possession. The meaning of the term "trade secret" is not limited to so-called "crown jewels", but potentially covers a very broad range of information held by a company as long as the requirements for protection (see below) are fulfilled.

A wide variety of information can qualify as trade secrets. These include different types of technical information (e.g. designs, drawings, architectural plans, blueprints and maps, algorithms, instructional methods, manufacturing or repair processes, techniques and know-how, document tracking processes, formulas for producing products) as well as business information (sales and distribution methods, lists of suppliers and clients and consumer profiles, business and advertising strategies, marketing plans, financial information). Even "negative" information as to "what does not work" or works less well could qualify as a trade secret.

Secrecy is, naturally, an essential requisite for a trade secret in all jurisdictions recognising such protection. Such secrecy generally is not required to be absolute but its dimension can differ from jurisdiction to jurisdiction, as can other requirements for protection.

The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS, 1994) obliges WTO member countries to protect undisclosed information providing it meets all the requirements below:

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

(c) It has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.[4]

The EU Directive also defines a trade secret as information which meets these three requirements,[5] and clarifies that "trivial information and the experience and skills gained by employees in the normal course of their employment" and "information which is generally known among, or is readily accessible to, persons within the circles that normally deal with the kind of information in question" may not be claimed as a trade secret.[6]

4 See TRIPS Section 7, Art. 39.

5 See Directive, Art. 2.

6 See Directive, Recital 14.

In the US, similar principles have existed under common law and are also reflected in state and federal legislation—at the state level, mainly the Uniform Trade Secrets Act (UTSA), and at the federal level, the DTSA.

In essence, the characteristic qualities of a trade secret are its secrecy, its value, and measures aimed at maintaining its secrecy.

2. Legal protection of trade secrets; comparison to other IP rights

The TRIPS Agreement obliges WTO member countries to protect undisclosed information meeting certain requirements, so as to empower "natural and legal persons to prevent 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".[7]

While many countries protect such undisclosed information under general unfair competition laws, specific trade secret legislation was introduced in 2016 in the EU (Trade Secrets Directive) and at the federal level in the US (Defend Trade Secrets Act, DTSA). The latter amended the 1996 Economic Espionage Act (EEA) to create a private right of action for misappropriation of trade secrets related to interstate or foreign commerce, without displacing state trade secret law.[8]

Unlike registrable industrial property rights — such as patents, utility models, trademarks and designs — trade secrets are typically protected without any procedural formalities. There is no need for patent-type novelty, industrial applicability or usefulness, or inventive step for information to be protected as a trade secret. Likewise, there is no need to fulfil the originality requirement applicable to copyright, and trade secrets may even be made up of components in the public domain which, if combined in ways not "known to or readily ascertainable by" a relevant public, can provide a competitive advantage and render the information valuable and proprietary.

While publicity is mandatory or can be of great benefit for trademarks and patents or copyrights, public disclosure inevitably leads to the loss of trade secret protection. However, trade secrets can be protected for an unlimited period of time, whereas registered rights (except for trademarks, which can be renewed periodically and indefinitely, but are subject to a genuine use requirement) and copyrighted works are protected for a limited period of time only. Trade secret protection is often a preferred alternative for products and processes that are difficult to reverse engineer, or that are not patentable but provide enterprises with a competitive advantage, or when patent protection is slow to obtain or too costly—though implementing many of the measures needed to protect a trade secret can also be expensive and time consuming. In general, small and medium-sized enterprises tend to rely much more on secrecy than on patenting.

7 See TRIPS, Section 7, Art. 39.

8 The Uniform Trade Secrets Act (UTSA, 1979) has been enacted in substantial form by all States except Massachusetts and New York.

Trade secrets are not qualified as intellectual property rights in the EU Directive—resulting in the non-applicability of the Enforcement Directive[9] to trade secrets, although individual Member States, notably Italy and Slovakia, have decided otherwise. The practical relevance of this inconsistency is limited in that the Trade Secrets Directive stipulates an enforcement regime quite similar to that of the Enforcement Directive.

In US practice, although trade secret protection is founded on notions of unfair competition by misappropriation, and although it does not prevent independent discovery and thus "ownership" by others, a trade secret is considered an intellectual property right which can be sold, licensed and taxed.

9 Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights.

III. Identifying and managing trade secrets; guidance for businesses

In order for a business to protect its trade secrets, it must first understand what that information is, how it contributes to the value of the company's products or services, and what the risks are of its disclosure, misuse or contamination. The responsibility for the management of this process lies initially with the business unit or function that generates this information asset. Any confidential business information that provides a competitive edge should be identified, at least by type, and then subjected to security protocols that are proportional to its perceived value and risk.

1. Identification of trade secret assets

The review of a company's valuable information assets to determine what qualifies as a trade secret is an important first step in the sensible management of those assets, whether they will mature into patent applications, be held for internal (secret) exploitation, or commercialised through partnerships or licensing.

From this knowledge base, a strategy and management system may be constructed. Typically this will be a cross-disciplinary process, involving managers of the relevant business units and functional areas such as legal and/or IP, human resources, IT and supply chain. Following an initial effort to identify and categorise key risks and to design systems at a high level, continuing management is usually assigned to a single executive with robust reporting responsibilities. Regular reviews are undertaken by the organisation's risk management and compliance practices.

Unlike some forms of intellectual property, trade secrets are not registered or otherwise described in a government filing. They reflect the value of information that has been maintained in secret by a business but that may be shared in confidence with employees or with third parties who are in a confidential relationship. As a practical matter, businesses need to have a general understanding of the types of information they possess which may qualify for protection. And in relationships where the information is shared, it is often important to provide notice of specific information considered as confidential. For some trade secrets, it is in the context of a dispute that they are first defined and described in detail.

The following guidelines help to determine whether any given set of information can qualify for protection.

a. General factors

Factors used to help determine whether information could be a trade secret include:

- The value of the information, as measured by the relative advantage it provides or by the harm that would be caused by its disclosure or misuse;
- The extent to which the information is distinct from individual skill or general knowledge, neither of which is protectable as a matter of public policy;
- The extent to which the information is protected against unauthorised access or misuse, both by insiders as well as by third parties (see "reasonable steps" below);

- The investment, effort, and money spent by the company to develop the information; and
- The ease of ability of others to independently generate, duplicate, reverse engineer, or acquire the information.

The lawful holder or owner of a trade secret (i.e., the person or entity that created and/or controls the information and its related documentation) is the one to perform in the first instance the identification and determination as outlined above. Whether the information is a trade secret or not ultimately may be decided by courts on a case-by-case basis and depends on an assessment of circumstances such as the factors listed above. The broad definition of trade secrets does not permit an approach governed by rigid rules, in part because only the trade secret owner can determine relative value and threats to secrecy, thereby setting priorities and adopting techniques to mitigate risk. That said, certain legal requirements merit emphasis.

b. Specific legal requirements to be taken into account when identifying trade secrets

Commercial value

To qualify as a trade secret under current US and EU law, information must have some commercial value, whether actual or potential. "Potential" value may exist even if the information has not yet resulted in a commercialised product or service, or if the information comprises failed experiments or other "negative" information, typically resulting from research, that can help point the way toward success. As already noted, value can be reflected in the extent of competitive advantage that the information provides, or in the harm that would result from improper acquisition, use or disclosure.[10]

There is no minimum value threshold, not least because the value of information is often very difficult to determine and may continually change. In practical terms, any perceived benefit is likely to qualify. It is worth noting that trade secrets need not be exclusive: even if the information may be known and applied by other firms, as long as it is not generally known, there may be value in the fact that a company's competitors do not know that it possesses the information.

Reasonable steps to preserve secrecy

TRIPS provides as a third qualification for "undisclosed information" to be protected that it be "subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret".[11] The EU Directive uses identical language to TRIPS for its three requirements of a "trade secret", including for the third qualification of "reasonable steps".[12] Under the prevailing US state law (UTSA), the relevant phrase is "reasonable efforts", while under the federal DTSA the standard is "reasonable measures". The practical implication of all of these standards is the same, focusing on what is "reasonable" to expect a trade secret owner to do, in order to qualify for help from the courts to enforce its rights.

10 See, for example, Recital 14 of the Directive.

11 See TRIPS, Art. 39(2)(c).

12 See Directive, Art. 2(1).

In the EU and the US, reasonableness is a factual question that will be decided by a judge or jury in the context of evidence about "the circumstances" of a company's risk environment, balancing the value of the secret information, the threat of loss or contamination, and the cost of various measures to mitigate the risks. While "courts do not require that extreme and unduly expensive procedures be taken to protect trade secrets against flagrant industrial espionage"[13], they expect to see measures taken that are proportional to the information security risks of everyday commerce, including turnover of employees, external collaborations for research and development, and long international supply chains.[14] There seems to be no major difference between the reasonable or best practices in security efforts for the protection of trade secrets recognised in the EU and the US.

The owner's intention to preserve secrecy needs to be proven by its behaviour before a dispute arises. That is, the owner must have demonstrated that it has committed a level of attention and resources that is related to the value of the information and the risk of loss or contamination. Because information security risks typically are dynamic, companies are expected to review and adjust their protection measures as appropriate according to the changing environment.

2. Managing trade secret assets

The management of trade secrets should take into account the three criteria discussed above, and in particular the requirement to take reasonable steps to preserve secrecy.

a. Risk assessment

After identifying the types of information to be protected, a trade secret security program should identify the risk environment and mitigation measures appropriate to reduce the risk. Which trade secrets might be taken, used or disclosed without authorisation, why, how, and by whom? This review may encompass relevant management of the company and its external contractors, supply chain vendors or staff, or other external parties such as competitors. What is the value of the trade secret and the corresponding extent of measures to protect it?

Not all secrets or confidential information deserve the same level of protection. Value and risk vary according to individual business circumstances, and often change over time. Businesses therefore may establish a hierarchy of required protections that reflect these priorities.

b. Specific measures

Once the risk assessment has been completed, measures should be taken to safeguard the identified information according to the degree of risk and value identified, taking into account the "reasonable steps/measures" legal requirement. Such measures may include the following:

13 See UTSA § 1 Commissionners' Comment.

14 Even before the Directive, the EU Commission's European IPR Helpdesk provided an outline of "measures and best practices," as well as links to fact sheets on how to manage confidential business information and non-disclosure agreements. While not binding, these references provide guidance for companies to implement "reasonable measures" required for protection of trade secrets. See https://www.iprhelpdesk.eu/ .

Labelling protocols

In order to be better identified, documents and electronic files that contain trade secrets should (and may even be required by law) be labelled in a way that prominently conveys the fact that they are subject to confidentiality restrictions, including any notice of restricted access.

For internal documents, a single word or phrase may be sufficient. For documents that may be seen outside the company, a variation on the following notice might be applied: "This document contains [COMPANY'S] confidential and proprietary information and is protected by copyright, trade secret and other laws. Its receipt or possession does not convey any rights, either express or implied, including any right to reproduce, distribute, disclose its contents, manufacture, use or sell any embodiment of the information described. If you have received this document in error, disregard the contents, and return or destroy.".

For small and simple business environments it may be sufficient to designate records in one category of protection, such as "confidential" or "secret"; in larger organisations, where information must be shared more widely, greater discernment may be required. In order to signal increasing levels of protective effort, multiple categories reflecting different levels of secrecy (e.g. "confidential", "secret", "trade secret") may be adopted, carrying different labels and controls, such as numbering and watermarking. However, all protocols should be sufficiently simple and intuitive for persons coming into contact with the information to understand the limitations on their access and use. If the term "trade secret" is used, the label should indicate that this categorisation does not imply that other information labelled differently is disqualified from trade secret protection.

Physical and electronic safeguards

Possible security safeguards include:

- *Restricted internal physical and electronic access:* Access to sensitive information should be limited to those with a need to know it, by physical means (for example, segregated secure facilities) or electronic systems that control multiple levels of access—preferably with multi-factor authentication—and that use monitoring software to alert management to high-risk behaviours.
- *External system protections:* Computer system intrusions by hackers seeking access to company secrets are increasingly common. There is a wide range of cybersecurity products and services available to erect defences and provide early warning of attacks. In addition, employee training programs should emphasise basic information security hygiene, such as recognition and prevention of "social engineering" attempts by outsiders to gain access to employee credentials.

Relationship Management

The overwhelming majority of trade secret losses are caused not by hackers but by current or former employees or business associates (supply chain and collaboration partners) who have authorised access to information but improperly disclose or misuse it. Risk of loss through such breaches may be attenuated through education, clear notice of duties, and vigorous enforcement. Non-disclosure agreements (NDAs) are generally useful, but not always effective, if the information sought to be protected is not reasonably identifiable or not treated as secret.

- *Employees:* In addition to requiring NDAs and, where possible, non-competition agreements (NCAs), employees and managers should be periodically trained on their duties to maintain secrecy of specific classes of information. Breaches should be met with serious disciplinary action that is reported for its educational effect. Hiring employees, particularly from competitors, should be done in a way that ensures no third party information is illegally brought into the company. This may require special training and continuing management attention. For departing employees, exit interviews can serve both to uncover potential breaches and to remind the departing employee of continuing obligations to keep information secret.
- *Third parties*: Whether dealing with vendors, customers or collaboration partners, sharing information in external relationships is often inevitable but fraught with risk. That risk can be mitigated in part by paying close attention to contracting, particularly terms that define information that must be kept secret, notice provisions, and the details of security measures expected of the other party and its employees. Where transactions call for joint development, it is critical to delineate ownership of information that is gathered or created during the project. But just as important as careful contracting is robust day-to-day management of the relationship. Compliance must be monitored, audits must be performed, and problems must be addressed as they arise. Since most information loss occurs through negligence or misunderstanding, active management can help to avoid disputes.

i. **Recommendations concerning specific types of information**

Below are some common examples of valuable information worth protecting by trade secret security programs, along with possible measures to safeguard that information:

- *Scientific and technical research, protocols and data, secret formulas, and computer code:* These are the archetypes of trade secrets, often the "crown jewels" of a business. Recommended measures include:
  - Marking documents and electronic files as "Trade Secret" or a similar legend, watermarking the most sensitive records;
  - Limiting access to information on a "need to know basis", including through the use of system access controls and monitoring; and
  - Providing on-going training for relevant staff on secrecy measures, with regular testing and evaluation.
- *Financial and accounting information:* In addition to marking records secret and compartmentalising the information, care should be taken not to expose more information than necessary for reporting purposes.
- *Marketing strategies and customer information:* While specific company strategies should be protectable, it is sometimes difficult to separate customer information from the general "skill, knowledge and experience" that an employee may use after termination. Customer lists with more detailed information are more likely to be protected. NCAs may be used in jurisdictions where they are permitted, as a way to reduce risk, particularly for information that degrades in value with time.
- *Public-facing information or products:* A basic principle of trade secret law in the US and in the EU, with notable exceptions such as Germany, is that reverse engineering of a publicly available product—for example, by disassembling it to see how it works—cannot

be considered misappropriation (see chapters V.4 and VI.4.a)). Although in the US and pursuant to the Directive this right to reverse engineer may be limited by contract in some circumstances, where goods (including software) are widely distributed, such a limitation may prove impractical, if not unenforceable under local laws. In one sense, this vulnerability of secret information reflects the general weakness of secrecy in comparison to patents, which provide exclusionary rights. As a result, trade secret holders need to develop their marketing and distribution strategies in a way that addresses information vulnerability. For example, companies relying on proprietary software tools increasingly place them in the cloud, where customers have access only to the results of processing their data, not to the tool itself.

IV. What constitutes misappropriation (infringement) of a trade secret

Because the EU Directive was designed to align with Article 39 of the TRIPS Agreement, which in turn was based on principles of US law (the UTSA), it is no surprise that the definition of "misappropriation" is substantially identical in the US and the EU.[15]

In the EU, Article 4 of the Directive defines misappropriation as the "unlawful acquisition, use or disclosure" of trade secrets.

The *acquisition* of a trade secret without consent of the trade secret holder is considered unlawful when it occurs by unauthorised access to, appropriation of, or copying of documents, objects, materials, substances or electronic files which contain the trade secret and which are lawfully under the control of the trade secret holder, or by any other conduct that is "contrary to honest commercial practices".

The *use or disclosure* of a trade secret is held unlawful whenever (a) the trade secret has been unlawfully acquired, or (b) such action constitutes a breach of a contractual or other duty not to disclose or limit the use of the trade secret, and occurs without consent of the trade secret holder.

Unlike as originally proposed by the EU Commission[16], intent or negligence are, in principle, not required elements of any misappropriation of a trade secret. This means the legitimate trade secret holder can obtain an injunction against an infringer regardless of fault. Claims for damages, in contrast, require that the infringer knew or ought to have known that it was engaging in a misappropriation of a trade secret.[17]

The acquisition, use or disclosure of a trade secret obtained from a third party, as well as the production, offering or placing on the market of infringing goods, or the importation, export or storage for those purposes, are deemed unlawful under the Directive only if the person concerned knew or ought to have known that the trade secret had been used or disclosed unlawfully.[18]

Under US legislation, the same division between acquisition and misuse or disclosure applies. Unlawful acquisition is defined in terms of "improper means", a phrase that has been given broad and flexible meaning by the courts and can be considered the equivalent of behaviour "contrary to honest commercial practices". This certainly includes hacking and all other forms of espionage, and it just as certainly does not include "proper" means such as independent discovery or reverse engineering.

---

15 See UTSA § 1(2); DTSA, 18 U.S.C. § 1839(5). In the two states, New York and Massachusetts, that have not adopted the UTSA, the common law definition of misappropriation is substantially the same.

16 See Art. 3, para. 2 of the Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, COM(2013) 813 final, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013PC0813&from=EN .

17 See Directive, Art. 14.

18 See Directive Art. 4, pars. 4 and 5.

If someone in possession of a trade secret knows that it was acquired by improper means or that it is subject to an obligation of confidence, then any unauthorised disclosure or use is an act of misappropriation. In this context, constructive knowledge may be imputed from the circumstances, so that the requirement in practice is not actual knowledge, but that the actor "knew or should have known".

The issue of "negligent" or "accidental" misuse or disclosure is treated somewhat differently under US law, but ultimately to the same effect as in the Directive. While there can be no liability in the absence of actual or constructive knowledge, once the actor receives notice that the information is a trade secret belonging to another person, liability attaches prospectively. However, if the accused can demonstrate that the information has in good faith been incorporated into a business process such that it would be unfair to enjoin continuing use, the court may in such exceptional circumstances decline the issuance of an injunction and instead impose a continuing royalty payable to the trade secret holder.[19]

19 See UTSA § 2(b).

V. Exceptions from protection

Under both US law (state law and the federal DTSA) and the Directive, there are certain exceptions and exclusions to the protection of trade secrets. Unlike the protections that exist for patents, if a competitor independently discovers the trade secret, or is able to learn the trade secret through reverse engineering of the relevant product, such conduct (absent an enforceable contract not to reverse engineer) does not infringe the trade secret holder's rights. Similarly, both the US law and the EU Directive place certain limits on employee non-compete agreements, even where it appears "inevitable" that the employee might disclose or use the trade secret. And employers are similarly restricted in using trade secret law to prevent employees from reporting unlawful conduct (whistleblowing). The Directive, however, provides more expansive exceptions where disclosure of the trade secret was carried out in exercise of freedom of expression, or for protecting "legitimate interests" recognised by the European Union. While these special exceptions are based on public policy concerns, their application may create opportunities for abuse if not properly limited to the specific circumstances that founded the concerns.

1. Employee rights

The EU has established employee rights to information and consultation through Article 27 of the Charter of Fundamental Rights of the European Union (CFREU) and through a number of directives.[20] The Trade Secrets Directive seeks to balance the rights of employees with the rights of companies to protect trade secrets. On the one hand, it should not affect agreements between employers and employees restricting competition between them,[21] while on the other hand, it should not prejudice the mobility of workers.[22] Trade secrets protection may therefore not extend to the skills acquired by workers during the course of their professional careers. Likewise, trade secret rights may be regulated and limited in the context of the exercise of workers' collective rights[23].

Most trade secret litigation **in the US** involves employees or former employees. Many of these cases also involve enforcement of non-competition agreements. Most US states, with the leading exception of California, enforce such agreements if they are reasonable in time, geography, and scope to protect legitimate interests of the employer and comply with local legal requirements. Typically, trade secret rights are considered a legitimate interest supporting such an agreement, even if it was signed after employment and the continued employment is "at will" (i.e., when the employee can be dismissed by the employer for any reason and without warning, if the reason is not illegal).

In general, departing employees are entitled to use "general knowledge, skills and experience" acquired in their employment. There have been a few cases applying US state law that enjoined for a relatively short period of time a former employee from working in a similar

20 Including Directives 2002/14/EC (establishing a framework for workers' right to information in order to promote social dialogue), 2001/23/EC (regarding safeguarding employees' rights in the event of transfers of undertakings and business), and 98/59/EC (regarding the laws of Member States on collective redundancies).

21 See Directive, Recital 13.

22 See Directive Recital 21.

23 See Directive, Recital 18.

position with a competitor on the grounds that the employee would "inevitably disclose [use]" confidential competitive information in such a position, based only on the employee's intimate knowledge of the trade secret. The DTSA, however, rejected this theory of "inevitable disclosure" and requires proof of behaviour demonstrating threatened misappropriation before limits may be placed on subsequent employment.

2. Whistleblowing activities

In the EU, the Directive creates an exception to trade secret protection for (i) revealing misconduct, wrongdoing or illegal activity for the purpose of protecting the general public interest; and (ii) disclosure by workers to their representatives as part of the legitimate exercise by those representatives of their functions[24].

This exception is consistent with the recent trend within the EU to protect informants, partially motivated by some high-profile cases. For example, the European Parliament requested in 2013 the submission of legislation that would establish an efficient and comprehensible program for the protection of informants in the public and private sector. The European Commission also issued a Communication on "further measures to enhance transparency and the fight against tax evasion and avoidance" in 2016.[25] In the second communication, the Commission highlighted the importance of improving protection for informants against the exposure to which they are subjected when they publish information considered to be secret.

In the US, prior to passage of the DTSA, a few courts recognised a limited and poorly defined public policy privilege to disclose trade secrets. The DTSA, however, expressly grants immunity to individuals who in confidence reveal trade secret information to government officials or their own attorneys for purposes of investigating corporate misconduct, or who disclose secrets in a sealed court filing.[26] This is the only provision of the DTSA that pre-empts state law.

The DTSA's whistle-blower protection is aimed at encouraging individuals with knowledge of wrongdoing to report to the authorities without fear of claims for violation of their NDAs. By conferring immunity only on disclosures made *in confidence* to either government officials, who are bound by state and federal law to protect trade secrets, and attorneys, who are bound by confidentiality obligations, the provision strikes a balance between protecting the interest of law enforcement in exposing illegal activity and the statute's general respect for private trade secret rights.

The most striking difference between the whistle-blower protections provided by the Directive and by the DTSA is that the latter extends only to confidential disclosures to government officials, while the former appears to approve of any disclosure made "for the purpose of protecting the public interest" potentially including public disclosure through the news media. However, the preamble to the Directive (Recital 20) suggests some limitations on such a broad interpretation: first, the information must be "directly relevant" to the misconduct; and second, the actor must have "every reason to believe in good faith" that the exception applies. To establish this exception without creating threats to the integrity of the very assets the Directive

24 See Directive, Art. 5(b), (c).

25 See COM/2016/0451.

26 See DTSA, 18 U.S.C. § 1833(2).

was intended to protect, courts may interpret it as being limited to disclosures in confidence to agencies capable of pursuing criminal prosecution.

3. Freedom of expression

In the EU, Article 5 of the Directive sets forth an exception to trade secret enforcement where the alleged acquisition, use or disclosure of the trade secret was carried out to exercise the right to freedom of expression and information as set out in the Charter of Fundamental Rights of the European Union (CFREU), including respect for the freedom and pluralism of the media. Freedom of expression is protected at the EU level in Article 11 of the CFREU, and comprises both the right of the issuer to express ideas, opinions and judgment, and also the right of the recipient to receive them. The importance of the protection of this right is reinforced in Recital 19 of the Directive, which recalls that despite the protections for trade secrets, "it is essential that the exercise of the right to freedom of expression and information which encompasses media freedom and pluralism [...] not be restricted, in particular with regard to investigative journalism and the protection of journalistic sources."

In the US, no similar exceptions to permit freedom of expression are to be found in trade secret law. The constitutional protection for freedom of speech is attenuated for "commercial speech" (in contrast to political speech). The 1996 Communications Decency Act (CDA) favours interactive computer service providers by immunising them for speaking or publishing the content provided by others but does not apply to limit "any law pertaining to intellectual property." The DTSA expressly states that it may not be construed as a "law pertaining to intellectual property for purposes of any other" federal law.[27] Thus, to the extent that immunity for trade secret disclosure may exist under the CDA (a notion that has not yet been tested in the courts), the DTSA would not change that result.

4. Independent discovery and reverse engineering

In the EU, Article 3 of the Directive provides that acquisition of a trade secret is lawful when accomplished through independent discovery or creation, or through observation, study, disassembly or testing of a product that is available to the public or lawfully in the possession of the acquirer without contractual prohibitions against such use. Recital 16 of the Preamble explains that this rule against exclusivity is provided "in the interest of innovation and to foster competition". The Directive goes on to note that in some industry sectors where products are subject to parasitic copying, national laws on unfair competition can address those practices. In contractual relationships the parties may prohibit reverse engineering of the other party's technology, but the Directive allows the Member States' legislators to restrict that option when they implement the Directive into national law.

Like the EU legislation, under both the UTSA and the DTSA, "misappropriation" is defined in **US legislation**, to exclude the discovery of a trade secret through independent invention or reverse engineering of a publicly available (and properly acquired) product. In this context, "independent" discovery or derivation requires that those doing the work have had no exposure to the information as a trade secret, so that the effort can be compared to the "clean

27 This should not be taken to mean that Congress did not consider trade secrets to be an intellectual property right. In fact, the first sentence of the Senate Report on the DTSA reads "Trade secrets are a form of intellectual property".

room" process of semiconductor manufacture, in which the fabrication environment is free of contaminants. In commercial transactions, the right to reverse engineer may be limited by the contract through which the actor gained access to the product. However, the application of this principle to consumer purchases is less settled.

5. Legitimate interests

The **EU Directive** creates an exception where the alleged acquisition, use or disclosure of the trade secret was carried out "for the purpose of protecting a legitimate interest recognised by Union or national law." The related Recital 21 clarifies that the exception is intended to enforce proportionality in issuing remedies for infringement so that they do not "jeopardise or undermine [...] the public interest, such as public safety, consumer protection, public health and environmental protection [...]". It goes on to explain that this exception is designed to ensure "that competent judicial authorities take into account factors such as the value of a trade secret, the seriousness of the conduct resulting in the unlawful acquisition, use or disclosure of the trade secret and the impact of such conduct. It should also be ensured that the competent judicial authorities have the discretion to weigh up the interests of the parties to the legal proceedings, as well as the interests of third parties including, where appropriate, consumers." Thus, rather than indicating a broad right of private actors to misappropriate in what they perceive to be the public interest, the exception instead expresses the fundamental notion that trade secret rights are not absolute, and that courts, in issuing orders for enforcement, are required to weigh and balance potentially competing interests.

While not codified as an exception, trade secret jurisprudence **in the US** has allowed similar accommodation of the public interest that can in appropriate circumstances override the private interests of the trade secret holder. This implementation of proportionality is most obvious in actions for injunctions, particularly in advance of trial, where courts are required to balance legitimate competing interests. For example, in a case involving computer software provided to a hospital, the court forced the trade secret holder to provide confidential access to the hospital's third party services vendor, recognising a public health interest that superseded the supposed rights of the trade secret holder. [28]

28 See Detroit Med. Ctr. v. GEAC Computer Sys., Inc., 103 F.Supp.2d 1019, 1024 (E.D. Mich. 2000).

VI. Enforcement of a trade secret

Formal enforcement of a trade secret requires a trade secret holder to initiate legal proceedings against an accused infringer, or "misappropriator". In such proceedings, the trade secret holder must establish the existence of, and its rights in, the trade secret, misappropriation of the trade secret, and its entitlement to one or more remedies, which are addressed in Chapter VII.

1. Elements of a misappropriation claim; burden of proof

The EU Directive instructs Member States to provide for the availability of measures, procedures and remedies to prevent, and to obtain redress for, the unlawful acquisition, use or disclosure of the trade secret.[29] The Directive is silent on the burden of proof but an applicant can expect to be required to provide reasonably available evidence to establish with a sufficient degree of certainty that (a) a trade secret exists, meaning that the requirements for protection under the Directive are fulfilled, (b) the applicant is the trade secret holder and (c) the trade secret has been or is being unlawfully acquired, used or disclosed, or an unlawful acquisition, use or disclosure of the trade secret is imminent.[30]

In deciding whether to grant or reject an application and in assessing its proportionality, the competent judicial authorities must take into account the specific circumstances of the case, including, where appropriate: (a) the value and other specific features of the trade secret; (b) the measures taken to protect the trade secret; (c) the conduct of the respondent in acquiring, using or disclosing the trade secret; (d) the impact of the unlawful use or disclosure of the trade secret; (e) the legitimate interests of the parties and the impact which granting or rejecting the application could have on the parties; (f) the legitimate interests of third parties; (g) the public interest; and (h) the safeguard of fundamental rights.[31]

In a civil case **in the US**, the trade secret holder bears the burden of proving, at trial or in a proceeding for special pre-trial relief, each element of the claim by a preponderance of the evidence. The plaintiff must show that the information is in fact secret, that the information derives its value from that secrecy, and that reasonable efforts have been made to protect the information. Misappropriation, through unauthorised acquisition, disclosure or use, can be shown by circumstantial evidence. For example, if the plaintiff proves that the defendant had access to the secret and that it was able to come to market with a suspiciously similar product or process in a short time, that may be enough to cause the burden to shift to the defendant to come forward with evidence of independent development. If the plaintiff seeks an injunction, the plaintiff does not need to demonstrate that misappropriation has already occurred; it is enough that it be threatened. "Threatened" misappropriation can be established through circumstantial evidence from which reasonable inferences can be drawn. In considering damages, courts will reject evidence deemed speculative, but so long as the likelihood of damage is reasonably certain, they tend to resolve in favour of the plaintiff any uncertainty regarding the amount to be awarded.

29 See Directive, Art. 4.1.

30 See Directive, Art. 11.1.

31 See Directive, Art. 11.2.

To initiate a case in the US, the plaintiff need not collect and present all the evidence necessary to establish a claim at trial. Indeed, because trade secret misappropriation often occurs without the plaintiff being aware of many underlying details, courts generally require, at the outset, only that the plaintiff submit basic allegations demonstrating a "plausible basis" for misappropriation. Whatever additional information the plaintiff needs to prove its case will normally become available through "discovery." Each side is permitted (under appropriate confidentiality restrictions) to have access to the other side's records and to examine under oath relevant witnesses, including non-parties to the litigation. Since enactment of the DTSA in 2016, trade secret holders still may bring their claims in state court, as before, but federal court may now be a more viable option in many cases so long as the claimed trade secret relates to a product or service intended for use in interstate or foreign commerce.[32]

2. Access to and assembling evidence

Again, this is a matter where the **EU Directive** refers to the procedural rules of the Member States. The plaintiff or applicant should examine these rules carefully in cases where the critical evidence is in the hands of the alleged infringer. The Member States apply different procedures—some of which work more effectively than others—but all have in common an intent to strike a balance between the interest of the plaintiff to gain access to evidence and the legitimate interests of the alleged infringer to maintain the secrecy of his or her own valuable information.

US procedural law assumes that a trade secret plaintiff may not be able, at the beginning of a case, to assemble the evidence required to prove a claim at trial. Therefore, an action can be initiated with a complaint that alleges sufficient information to establish that its claim is reasonably plausible. At this pleading stage, some courts demand a particularised statement of the trade secrets at issue, while some others are satisfied with a categorical description that informs the defendant in general terms about the substance of the claim. After the pleadings are settled, litigants are entitled to seek broad discovery from each other, in both written and oral form. Notably, under US law, parties are required to preserve evidence that may relate to any impending legal suit, even absent a court order or request from the opposing party. Once a suit is filed and formal discovery begins, written discovery primarily focuses on the exchange of relevant records, whether physical or electronic, including emails, text messages and all other forms of communication. Often, access is provided to computer systems in order to search for evidence, although this typically is done only under expert supervision. Parties may also request to inspect physical facilities of the opposing party. Once the majority of written evidence is exchanged, the parties begin to elicit sworn testimony from witnesses. Although this process happens outside of the presence of the judge, it is supervised by the court and may be used as evidence in the proceedings.

Having collected "fact" evidence through the discovery process, the parties then often submit reports prepared by their respective, party-retained experts, who explain technical or economic issues. In contrast with virtually all civil law systems, the evidence, including expert testimony, is usually presented to a jury of ordinary citizens, who determine, for example, whether misappropriation has occurred and, if so, the amount of any damages award. Notably, much of the evidence may have already been presented to the court earlier in the case in order to support a request for extraordinary relief, such as seizure of accused products or an

32 See DTSA, 18 U.S.C. §1836(b).

interim injunction. As explained below, during the entire effort to gather and sort the evidence, confidentiality of certain evidence, such as the claimed trade secret, is typically protected by a court order that prohibits disclosure or use of such evidence outside of the litigation process.

3. Admissibility of expert evidence

With respect to the role of experts, the **EU Directive** defers to the laws and practice of the courts in Member States. Those laws and practice vary significantly within the EU and hence the admissibility and use of expert evidence also vary significantly. For example, party-appointed experts are prevalent, but in some Member States, oral expert testimony is permitted (including with cross-examination) while in others only written expert testimony is received. Further, in some Member States, experts can be engaged by the court, whereas in others this is not possible. The areas of expertise vary, but may include technical issues (e.g. relating to the substance of the trade secret), forensics (e.g. relating to the manner/extent of acquisition/use/disclosure) and accounting or financial matters (e.g. relating to the damages arising from the misappropriation).

In the US, experts are frequently called as witnesses to provide opinions on various trade secret issues, such as the substance of the claimed trade secret (for example, whether it is or is not generally known), its value, the reasonableness of efforts to maintain confidentiality, and the fact and amount of damages sustained by the plaintiff as a result of the misappropriation. Increasingly, forensic experts are called to explain how certain evidence was hidden or destroyed or to explain other aspects of computer and communications technology. Because these questions are often beyond the common experience of judges and juries, courts will accept expert testimony to the extent it is helpful in resolving those questions, so long as the expert witness has sufficient "knowledge, skill, experience, training or education" and his/her opinion is grounded in scientifically reliable analysis. Although opinions are sometimes received from a neutral expert appointed by the court, it is much more common for the parties to present, and pay for, their own experts, reflecting the adversarial system of US dispute resolution.

4. Elements of certain defences

a. Reverse engineering

In the EU, the acquisition of a trade secret shall be considered lawful when the trade secret is obtained by observation, study, disassembly, testing or otherwise analysing a publicly available product or object to discover how it works or how it was made.[33]

As is the case in the EU, reverse engineering is deemed a proper method of acquiring a trade secret under **US law**. Indeed, if the defendant is able to prove that the reverse engineering process is or would be relatively quick (e.g. as short as a few days), then courts may find the information to be "readily ascertainable" and so trivial that it cannot be a trade secret. However, the fact that a trade secret is capable of being reverse engineered is not sufficient to excuse a person who failed to actually reverse engineer and instead misappropriated the trade secret. In such a case, the court might limit damages or an injunction period to the "lead time"

33 See Directive, Art. 3.1 (b).

or "head start" that the plaintiff should have enjoyed. Finally, successfully establishing a reverse engineering defence requires the defendant to prove that anyone working on the accused product or process had not previously been exposed to the trade secret.

b. Independent development

In the EU, as noted in Chapter V.4, a trade secret may be lawfully acquired through "independent discovery or creation".[34] The burden of proof is on the defendant to establish this fact.

Under US legislation, although a trade secret plaintiff always has the burden of proof, sometimes the evidence is so suggestive of misappropriation (for example, when a defendant was able to develop its competing product in record time) that, as a practical matter, the court expects to hear an explanatory story from the defendant. Therefore, almost all trade secret disputes include a substantial effort by the defendant to prove independent development or discovery. Simple cases involve demonstrating acquisition of the information from a third party that was not in a confidential relationship with the plaintiff. More often, the defendant submits its contemporaneous research and development or engineering records and explains how each major decision, result or discovery occurred. Since all of this information is presumably already available to the defendant, marshalling such proof is usually not difficult.

c. Other exceptions from protection

The defences mentioned above are outlined in more detail in Chapter V, dedicated to exceptions from protection. The other exceptions from protection discussed in Chapter V—employees' rights, whistleblowing, freedom of expression and legitimate interests—also serve as defences.

5. Preservation of confidentiality

EU Member States have to ensure that any person participating in legal proceedings, or who has access to documents involved in those proceedings, is prohibited from using or disclosing any trade secret that a competent judicial authority has—in response to a duly reasoned application by an interested party—identified as confidential and of which the person has become aware as a result of such participation or access.[35] Further, the competent judicial authorities may, on a duly reasoned application by a party, take other measures necessary to preserve the confidentiality of any trade secret or alleged trade secret used or referred to in the course of legal proceedings relating to the unlawful acquisition, use or disclosure of a trade secret.[36] Member States may also allow competent judicial authorities to act on their own initiative and to make available non-confidential versions of any judicial decision in which descriptions of trade secrets have been removed or redacted.[37]

34 See Directive, Art. 3.1 (a).

35 See Directive, Art. 9.1.

36 See Directive, Art. 9.2.

37 Idem.

Still, even in the absence of discovery measures prevalent in the US, the risk of a breach of confidentiality remains a barrier to effective judicial proceedings. The problem is that, in a number of Member States, procedural principles and requirements, such as the publicity of the proceedings (and often of the court files), and a reasonably detailed description of the trade secret as a prerequisite for an enforceable award, fundamentally contravene the concept of preserving the secrecy of the information. *In camera* proceedings, which would exclude the public and even representatives of the parties (except the parties' lawyers), could provide a solution, but are rarely available because of the dominating principle of publicity.

The Directive arguably fails to offer an effective remedy to that problem because it stipulates that at least one representative of each party, in addition to the parties' lawyers, may attend hearings. Orders obliging such representatives to preserve the confidentiality of the information obtained during a hearing may not always be an effective deterrent to using the information.

Bearing that in mind, confidentiality or non-disclosure agreements between the parties, including their lawyers, may be an effective, practical approach to preserve a trade secret's confidentiality. Examples of such an approach can be found in litigation relating to IP rights.[38]

It has already been noted that enforcement of a claimed trade secret through litigation may increase the risk of its unauthorised acquisition, disclosure, or use. During discovery **in the US**, each side is allowed access to the other side's relevant records. As part of that process, the parties seek from the court, sometimes by agreement, a protective order that allows each side to designate discovery materials that they wish to protect. Frequently, such orders will create two categories of protected information: (1) "confidential" information—limited to certain designated individuals; and (2) "highly confidential" information—limited to the parties' lawyers and qualified experts allowed to access such information. Once in possession of "highly confidential" information, the lawyers will be able to make informed arguments about the need for their clients, i.e., (a) designated client representative(s), to also have access to some or all of that information. In general, a protective order is an effective deterrent to improper acquisition, disclosure and use of protected information.

Once such information has been used in a proceeding on the merits of a claim, such as in a trial or on a motion for early (or "summary") judgment, materials filed "under seal" in the court may be exposed to requests for access by the media. In light of constitutional provisions that favour the press and open court proceedings, courts will normally deny those requests only if the owner of the information demonstrates a "compelling need"; in other words, the owner demonstrates not just that the information qualifies as a trade secret, but also that it is sufficiently important that its disclosure would cause real harm.

Once a trade secret dispute moves from the pre-trial discovery phase and into trial, management of secrecy becomes more complex. In addition to the parties and their counsel, court staff and juries will necessarily be exposed to confidential information and so must be instructed about their obligations of confidentiality. Even so, the more widespread exposure necessarily increases the risk of a loss of confidentiality, at a minimum through negligent behaviour.

38 See e.g. Oberlandesgericht Düsseldorf, 17.01.2017.

Finally, long-established practice and constitutional norms strongly favour court proceedings that are open to the public. Many judges are reluctant to close the courtroom to visitors and tend to be demanding about the sort of information that can justify closure. If such a step is taken, then secret evidence may be presented collectively to avoid interruptions to the trial. Despite all of these challenges, US courts have substantial experience protecting confidential information. Instances of information losing its confidentiality during litigation or trial where the trade secret owner has not openly disclosed it without restriction are rare. Courts also may take practical measures to protect trade secrets, such as requiring computer screens containing evidence to be turned away from public view or requiring witnesses and lawyers to refer to ingredients by code names in open court.

VII. Civil remedies

Generally speaking, a trade secret holder can seek two types of remedies in connection with enforcing its trade secret:

- Remedies that stop, or at least limit, the misappropriation and other wrongful activity, such as injunctions, seizure and measures to block importation; and
- Remedies that compensate the trade secret holder for the misappropriation, such as damages, fees and costs.[39]

1. Injunctions

Under the **EU Directive**, Member States shall ensure the availability of measures to prevent or prohibit the unlawful use and disclosure of a trade secret.[40] Such measures are to include provisional (i.e., pre-trial/prior to a decision on the merits) and final or permanent (i.e., post-trial) injunctions. In each case, the judicial authority may order the following measures against the infringer:

- cessation of or prohibition on the use or disclosure of the trade secret;
- cessation of or prohibition on the production, offering, placing on the market or sale of infringing goods, or the importation, export or storage of infringing goods for those purposes.

While the weight given to the factors that each Member State's judicial authorities consider when deciding whether to grant injunctive relief varies to some extent (in particular, based on respective procedural rules/practice), the Directive requires that judicial authorities take into account the specific circumstances of the case, as set forth in Chapter VI.1 above.[41]

Member States are also required to ensure that the competent judicial authorities may:

- revoke provisional relief or order that it cease to have effect, upon the request of the respondent, if: (a) the applicant does not timely institute legal proceedings leading to a decision on the merits of the case by the competent judicial authority; or (b) the information in question is no longer a trade secret (as defined by the Directive), for reasons not attributed to the respondent;
- condition provisional injunctive relief on the applicant providing adequate security or an equivalent assurance intended to ensure compensation for any prejudice suffered by the respondent and, where appropriate, by any other person affected by the injunctive relief; and
- where provisional injunctive relief (a) is revoked or ceases to have effect as provided above or (b) lapses due to any act or omission by the applicant, or where there is a subsequent finding that there has been no unlawful acquisition, use or disclosure of the trade secret or threat of such conduct, order the applicant, upon the request of the respondent or an injured third party, to provide the respondent, or the injured third party, appropriate compensation for any injury caused by the provisional injunctive relief.

---

39 For an overview and comparison of the civil remedies available in each EU member state (prior to the implementation of the Directive), see the EUIPO report *The Baseline of Trade Secrets Litigation in the EU* (2018) (pp. 348-360), https://euipo.europa.eu/ohimportal/fr/web/observatory/observatory-publications .

40 See Directive, Arts. 10.1 and 12.1.

41 See Directive, Art. 11.2.

Additionally, the Directive provides that Member States may permit an alleged infringer, subject to appropriate conditions, to continue to use an alleged trade secret, in particular where there is little risk that the alleged trade secret will enter the public domain through such continued use.

Under **US state or federal law**, judges have broad power to issue injunctions against continuing, threatened, or likely misappropriation. Injunctions issued before trial are viewed as an "extraordinary" remedy, requiring a strong showing of likely, irreparable harm, together with a balance of interests in favour of the moving party, and, where applicable, the public. An injunction normally may last only so long as the trade secret remains secret, although it may be continued for an additional period of time on a showing that a longer period is necessary to compensate the plaintiff for the lost "head start" period resulting from the misappropriation. Affirmative measures to protect trade secrets, including the appointment of compliance monitors, orders directing the return or forensic removal of documents and files, and on-going reporting requirements, are available under both state and federal law.[42] Notably, injunctions can be directed at conduct occurring outside of the US.[43]

Although the standards for obtaining an injunction are similar under state and federal law, the DTSA provides special protections for departing employees. In the absence of an enforceable non-competition agreement, federal courts may not prohibit an employee from accepting employment with a competitor. They may impose limitations (such as working in a lower-risk assignment for a period of time) only based on evidence of misbehaviour; mere knowledge of sensitive information is not sufficient.[44]

2. Seizure

Under the **EU Directive**, Member States shall ensure that judicial authorities may order the seizure or delivery up of suspected infringing goods, by way of, for example, provisional (i.e., pre-trial) measures.[45] The availability of such measures depends on the same analysis used for provisional injunctions, discussed in section 1 above.

In the US, pre-trial seizure, like an injunction, is considered an "extraordinary" remedy available only with strong evidence supporting the misappropriation claim and a clear balance of interests in favour of the trade secret owner. State laws vary considerably, with only a few states providing a seizure remedy, although individual states or judges may grant equivalent relief in the form of a "mandatory injunction". Under the DTSA, federal courts may issue seizure orders *ex parte* when it can be shown that the trade secret is in imminent danger of destruction or removal from the jurisdiction, but the requirements are strict, and the seized material may only be viewed and handled by officials and the court until a full hearing can be held.[46] Parties are, however, required to preserve relevant evidence for use in litigation.

---

42 See §1836(b)(3)(A)(ii); UTSA §2(c).

43 See, e.g., Restatement (Third) Unfair Competition §44, comment d (1995), citing Lamb-Weston, Inc. v. McCain Foods, Ltd., 941 F. 2d 970 (9th Cir. 1991).

44 See DTSA, §1836(b)(3)(A)(i)(I).

45 See Directive, Art. 10.1 (c).

46 See DTSA, 18 USC § 1836(b)(2).

3. Blocking importation

Under the **EU Directive**, Member States shall ensure that judicial authorities, among other provisional or precautionary measures, may prohibit the importation of infringing goods and the storage of such goods for the purpose of importation[47] and order the seizure or delivery up of infringing goods for such purpose.[48] The availability of such measures depends on the same analysis used for provisional injunctions, discussed in section 1 above.

Federal and state courts in the **US**, using their power to issue broad forms of injunctive relief, can prohibit parties from importing into the US goods made with, or that include, a trade secret. Another viable remedy against importation is available from the United States International Trade Commission (ITC), a specialised tribunal in Washington, D.C. that asserts jurisdiction over accused goods and often acts faster than most courts. Even where acts constituting misappropriation have occurred entirely outside of the US, the ITC can issue exclusion orders that will be enforced at the national borders by US Customs.[49] The ITC can also issue cease and desist orders prohibiting the transfer, distribution or sale of articles already imported into the US.

4. Damages (monetary awards)

The **EU Directive** requires Member States to ensure that the competent judicial authorities, if so requested by the injured party, order the payment of damages against the infringer who knew or ought to have known that it was engaging in the unlawful acquisition, use or disclosure of a trade secret.[50] Damages awarded shall correspond to the actual harm suffered as a result of the trade secret misappropriation.[51] Member States may limit an employee's liability for damages to the employer for misappropriation where the employee acted without intent.[52]

The determination of the amount payable by the infringer shall take into consideration the lost profits of the trade secret holder, unfair profits made by the infringer and, in appropriate cases, non-economic factors, such as the moral prejudice caused to the trade secret holder as a result of the misappropriation.[53] Alternatively, the competent judicial authority may, in appropriate cases, set the damages as a lump sum on the basis of elements such as, at a minimum, the amount of royalties or fees which would have been due had the misappropriator requested authorisation to use the trade secret in question.[54]

At the request of an infringer who neither knew nor ought to have known that he or she obtained the trade secret from a person unlawfully using or disclosing the trade secret,

---

47 See Directive, Art. 10.1 (b).

48 See Directive, Art. 10.1 (b) and (c).

49 See *TianRui Group Co. v. ITC*, 661 F.3d 1322, 1332 (2011).

50 See Directive, Art. 14.1.

51 *Ibid*.

52 *Ibid.*

53 See Directive, Art. 14.2.

54 *Ibid.*

pecuniary compensation may be ordered by the judicial authority instead of, for example, an injunction or destruction of the infringing goods.[55]

Under **US law,** damages for misappropriation reflect the tort law objective of full compensation to the victim. Three methods of calculation are generally available:

- Actual loss (typically lost profits, as well as development costs, and price or market erosion);
- Unjust enrichment, which may include avoided development costs; and
- Reasonable royalty.[56]

Each of these methods may be used in combination with the others, provided the combined damages are not duplicative compensation for the same harm.[57]

Exemplary damages—no more than twice the awarded damages—may be added by the court if wilful and malicious misappropriation is proved.[58]

Although damages are not available at the ITC, they are available through court proceedings that typically are filed concurrently with, but stayed during, an ITC proceeding.

5. Fees and costs

The **EU Directive** stipulates that, in the absence of particular reasons to the contrary, corrective measures, such as the destruction of documents, objects, materials, substance or electronic files which embody the trade secret, shall be carried out at the expense of the infringer. Otherwise, the recovery of costs is determined by the laws of each Member State. In general, recovery by the prevailing party of their attorney's fees and costs is permitted in the EU.

The applicant may be ordered by the competent judicial authorities to post an adequate security or an equivalent assurance to ensure compensation for any prejudice suffered by the respondent and, where appropriate, by any other person affected by provisional and precautionary measures applied for (discussed in Chapter VII.1 above).[59]

In the **US**, civil litigation costs (for example, filing fees and some discovery costs) are usually awarded to the prevailing party, but not attorney's fees. This rule, however, is varied in trade secret cases. Where the misappropriation is wilful and malicious, the court may award attorney's fees to the trade secret owner. Likewise, the court may award attorney's fees to the defendant where the misappropriation claim is without merit and made in bad faith.[60]

---

55 See Directive, Art. 14.3.

56 See DTSA, 18 U.S.C. § 1836(b)(3)(B); UTSA, § 3(a); *Roton Barrier, Inc. v. Stanley Works*, 73 F.3d 112, 119-20 (Fed. Cir. 1996), *reh'g denied* (1996); *Stanacard, LLC v. Rubard LLC*, 2016 WL 6820741, *1-3 (S.D.N.Y. Nov. 10, 2016).

57 See DTSA, 18 U.S.C. § 1836(b)(3)(B); UTSA, § 3(a).

58 See DTSA, 18 U.S.C. § 1836(b)(3)(C); UTSA, § 3(b).

59 See Directive, Arts. 11.2 and 11.4.

60 See DTSA, 18 U.S.C. §1836(b)(3)(C); UTSA, §4.

VIII. Limitation period for claims

Limitation periods set a time limit for bringing claims, thereby providing predictability and an incentive for victims to gather evidence and present claims while they are fresh. The EU and US trade secret legislations provide for differing limitation periods.

The **EU Directive** stipulates that the limitation period cannot exceed six years.[61] Other than that, EU Member States can impose their own rules on the limitation periods applicable to substantive claims and actions for the application of the measures, procedures and remedies provided for in the Directive. It is also for EU Member States to determine when the limitation periods begin to run, their duration and the circumstances under which they can be interrupted and restart from the beginning, or be suspended.

In the **US**, the law on the time for bringing claims is fairly uniform among the states and the federal system. Under the UTSA, the period for bringing claims is three years, but a few states have amended their laws to provide a longer time. Claims made under the DTSA also enjoy a three-year limitation period. Whether in state or federal court, the time typically begins to run when the trade secret owner "discovers" the misappropriation, or when in the exercise of normal due diligence it "should have" become aware of it. Most jurisdictions follow the "single claim" approach, in which the limitations period starts when the first act of misappropriation is discovered. Subsequent acts of misappropriation in the same relationship do not begin anew the running of the limitation period.

61 See Directive, Art. 8.

IX. Scope of territorial jurisdiction

The **EU Directive** does not address the scope of territorial jurisdiction:

> "This Directive does not aim to establish harmonised rules for judicial cooperation, jurisdiction, the recognition and enforcement of judgments in civil and commercial matters, or deal with applicable law. Other Union instruments which govern such matters in general terms should, in principle, remain equally applicable to the field covered by this Directive".[62]

Hence, the scope of territorial jurisdiction within the EU must be determined pursuant to the relevant provisions of the Recast Brussels Regulation,[63] or of the Brussels Regime[64] in general. Rules on unitary EU intellectual property rights (such as European Union trade marks) have their own jurisdiction regimes, which deviate from the Brussels Regime[65] and do not apply to actions under the Directive.

Pursuant to the Recast Brussels Regulation, persons domiciled in a Member State shall, whatever their nationality, be sued in civil and commercial matters in the courts of that country.[66] In principle, this also applies in the event that the plaintiff is domiciled in a third state.[67] A legal person is principally domiciled where it has its statutory seat, central administration, or principal place of business.[68]

Nonetheless, a person domiciled in a Member State may be sued in another Member State in matters relating to tort, delict or quasi-delict, namely in the courts for the place where the harmful event occurred or may occur.[69] This provision applies to non-contractual liability, including unfair competition and infringement of intellectual property rights. The defendant may be sued, at the option of the plaintiff, either in the courts of the place where the damage occurred or in the courts of the place of the event which gives rise to and is at the origin of that damage.[70]

---

62 See Directive, Recital 37.

63 Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast), replacing Regulation (EC) No 44/2001 of 22 December 2000.

64 According to an international convention (OJ L 299, 16/11/2005, p. 62; OJ L 79, 21/3/2013, p. 4), the provisions of the (recast) Brussels Regulation shall also apply to Denmark, for which the Regulation is not binding. The so-called Lugano Convention (Convention 88/592/EEC on jurisdiction and the enforcement of judgments in civil and commercial matters—done at Lugano on 16 September 1988, applies among EU Member States, Switzerland, Norway and Iceland and is essentially equal to the Brussels Regulation.

65 See, for example, Arts. 123 et seq. of Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark (codification) concerning the jurisdiction of EU trade mark courts.

66 See Recast Brussels Regulation, Art. 4 in conjunction with Art. 1.

67 See *ECJ* (Sixth Chamber), Judgment of 13 July 2000—*Group Josi Reinsurance Company SA v Universal General Insurance Company (UGIC)*—Case C-412/98.

68 See Recast Brussels Regulation, Art. 63 para. 1.

69 Recast Brussels Regulation, Art. 7 para. 2.

70 See *ECJ*, Judgment of 30 November 1976—*Handelskwekerij G. J. Bier BV v. Mines de potasse d'Alsace SA*—Case 21/76.

In general, a judgement founded on Article 4 jurisdiction (country where the defendant is domiciled) provides the possibility of a remedy regarding infringing acts wherever they have occurred in the EU.[71] In contrast, a court seized on the basis of the place where the alleged damage occurred (Article 7 para. 2) has in most cases jurisdiction only to rule on the damage caused within that Member State.[72]

The precedence of the Brussels Regulation over national legislation does not apply to provisional measures—a plaintiff may apply to the courts of a Member State for provisional measures available under the law of that Member State, even if the substance of the matter is under the jurisdiction of the courts of another Member State.[73]

A judgment rendered in a Member State shall be recognised in the other Member States without requiring any special procedure.[74] Likewise, a judgment rendered in a Member State which is enforceable in that Member State shall be enforceable in the other Member States without requiring any declaration of enforceability—the recognition or enforcement may be refused only if grounds for refusal apply.[75]

Under the **US federal system**, there are separate rules to determine whether state or federal courts may apply their law to reach misappropriation that occurs in whole or in part outside their jurisdictional borders.

States typically operate under so-called "long-arm" statutes that allow their courts to exercise jurisdiction more or less as allowed under the "due process" clause of the US Constitution. These general statutes apply to trade secret misappropriation cases, with the additional gloss that such cases, because they involve wrongful conduct, are more likely to be accepted when harm is alleged to have occurred within the jurisdiction.

Federal statutes are presumed not to have extraterritorial reach unless Congress has expressed a clear intent to do so. In enacting the DTSA, Congress did express a strong concern over foreign acts of misappropriation of US-based secrets, which it found necessarily cause economic harm within the country. However, it did not amend the pre-existing provision of the Economic Espionage Act that specifically addressed extraterritoriality[76] and limited it to cases in which an "offender" is a US citizen or at least one act in furtherance of the "offense" occurred in the US. It is not yet clear whether these restrictions will apply to cases filed under the DTSA, but traditional limitations based on due process should ensure that courts assume jurisdiction only in cases where there is a logical relationship of the jurisdiction to the alleged misappropriation.

---

71 See *Cook*, Territoriality and Jurisdiction in EU IP Law, Journal of Intellectual Property Rights, Vol 19, July 2014, p. 293 (294).

72 See *ECJ* (Fourth Chamber), Judgment of 22 January 2015—*Pez Hejduk v. EnergieAgentur.NRW GmbH*—Case C-441/13; *ECJ*, Judgment of 7 March 1995—*Fiona Shevill, Ixora Trading Inc., Chequepoint SARL and Chequepoint International Ltd v Presse Alliance SA.*—Case C-68/93; *Cook*, Territoriality and Jurisdiction in EU IP Law, Journal of Intellectual Property Rights, Vol 19, July 2014, p. 293 (294).

73 See Brussels Regulation, Art. 35.

74 See Brussels Regulation, Art. 36 para. 1.

75 See Brussels Regulation, Arts. 39 and 45 et seq..

76 See 18 U.S.C. § 1837.

In contrast, the ITC has authority to prohibit the importation of goods and domestic sales of previously imported goods, where such goods resulted from unfair methods of competition, including trade secret misappropriation, regardless of where in the worlds the wrongful behaviour occurred, and without regard to the limitations on jurisdiction under the Economic Espionage Act.[77]

77 See *TianRui Group Co. v. ITC*, 661 F.3d 1322 (Fed. Cir. 2011).

X. Criminal sanctions

The **EU Directive** allows Member States to subject acts of trade secret misappropriation to criminal sanctions, in addition to the measures provided under applicable civil law.

Almost half of the **US** states have enacted laws applying criminal penalties to the theft of trade secrets, although only a few states have actually prosecuted cases under those laws. In 1996, the federal government enacted its first such law, the Economic Espionage Act (EEA), in response to concern over foreign state-sponsored theft of trade secrets. However, the EEA is not limited to cases involving crimes committed on behalf of a foreign agency. It also applies to any trade secret theft affecting national commerce, so long as the offender is a US citizen or an "act in furtherance of the offense" occurred in the US. Criminal conduct can include an unsuccessful attempt to misappropriate, as well as participation in a conspiracy to do so. Penalties can be severe, with fines in the millions of dollars and years in prison for convicted individuals. Because cases brought under the EEA can be complex and difficult to prove under the heightened evidence standards of criminal cases, the Department of Justice has established a training program for specialist prosecutors, and each district includes at least one attorney assigned to oversee EEA matters. Because only the most serious cases can meet criminal prosecution standards, and because victims often prefer to use the civil courts and retain control over their cases, fewer than ten cases per year are filed under the federal statute. Prosecutions under state criminal trade secret laws have become rare since the enactment of the EEA. The DTSA also makes trade secret misappropriation a predicate offense for claims under the federal Racketeer Influenced and Corrupt Organizations ("RICO") statute, under which both civil and criminal penalties, attorney's fees, treble damages, and forfeiture of property derived from racketeering activity can be imposed upon a showing that defendant has engaged in at least two related acts of racketeering activity within a ten year period and that there is a threat of "continued criminal activity".[78]

78 See 18 U.S.C. §1961 (a)-(d).

XI. Aspects to consider in trade secret regimes: recommendations for policy makers worldwide

From a policy perspective, there is a need to balance the private interest in commercial secrecy with competing public interests. For example, the ingredients in drugs, pesticides and fertilisers should always be available to regulators as a matter of ensuring public safety. However, while great value is rightly placed on transparency in government and other public institutions, in the commercial realm there is no reason to view sceptically the general application of secrecy laws to protect investment in new products and processes. Indeed, trade secrecy is the oldest form of intellectual property, enabling the commercialisation of valuable innovations that otherwise might never reach the public. As increasing global sourcing and the expansion of businesses to high-growth markets increases the risk of unauthorised use of trade secrets and confidential business information, effective protection against misappropriation of trade secrets will also be increasingly important to encourage knowledge sharing and collaboration.

The OECD published a two-phase project comparing the regulatory regimes concerning trade secrets in different jurisdictions[79] and analysing their economic consequences.[80] The papers show, on the one hand, substantial differences with respect to implementation of protection for trade secrets and, on the other hand, evidence that there is more innovation in countries with higher trade secret protection. A notable increase in the stringency of trade secrets protection in a broad sample of countries during the period from 1985 to 2010 was found by the OECD to be positively associated with key indicators of innovation and international economic flows.[81]

For more technologically advanced economies, the general observation is clear enough: strong enforcement systems for trade secrets form a necessary component of any national innovation strategy. For countries wanting to move up the innovation ladder, the issue is even more compelling: the globalised, digital economy offers unprecedented opportunities for participation in international innovation, manufacturing and distribution networks, but only for those actors who can be trusted because they are subject to appropriate legal frameworks in their home jurisdiction. Countries that provide those frameworks will enjoy an increasing economic advantage from networked innovation.

The introduction of legislative frameworks specifically aimed at protecting trade secrets should be analysed on a country-by-country basis: the TRIPS Agreement provides a framework agreed among most countries of the world, which individual countries can use as a starting point, developing more specific provisions as appropriate to their existing legal structures and their national innovation strategies.

Drawing from the lessons learnt from a comparison of the US and EU approaches to the protection of trade secrets, below are the most salient global observations and suggestions to help guide policy makers worldwide on whether or how to establish or reform frameworks for trade secret protection.

79 See dx.doi.org/10.1787/5jz9z43w0jnw-en .

80 See dx.doi.org/10.1787/5jxzl5w3j3s6-en .

81 See www.oecd.org/sti/ieconomy/Chapter3-KBC2-IP.pdf .

Trade secrets as "intellectual property"

The EU decided, contrary to the recommendation of its 2013 study, not to make the IP Enforcement Directive applicable to trade secrets, by specifying that they may not be considered as "intellectual property rights". As a result, although the Directive tries to mirror the instruments stipulated in the IP Enforcement Directive in many aspects, it has had the effect of depriving trade secret holders of some of the key remedies that would have been available through the Enforcement Directive.

In contrast to the position taken by the EU in the Directive, the US has for many years considered that trade secrets, which can be licensed, sold and taxed, are a form of intellectual property. This recognition has helped reinforce judicial decisions protecting the rights of trade secret holders.

The TRIPS Agreement provides that all its enforcement and other cross-cutting provisions should apply to all the intellectual property rights it covers, including undisclosed information, or trade secrets. Thus, whether or not trade secrets are categorised as intellectual property rights in national legislation, they should benefit from a similar level of protection as other IP rights with respect, for example, to possibilities for enforcement. As seen from the EU and US examples, in some countries this could be ensured more effectively by treating trade secrets as a form of intellectual property right, though that may not be the case everywhere.

Access to proof of misappropriation

By its nature, trade secret misappropriation usually happens without the knowledge of the victim. Even when the trade secret owner discovers that a loss has occurred, it typically does not have access to direct evidence of who did it or how it was done. Instead, the owner must draw inferences from circumstantial evidence, for example of a rival's too-quick product development following its hiring of one of the owner's employees.

In the US, courts will accept such a circumstantial, but plausible, assertion as sufficient to begin litigation and secure "discovery" of evidence in the possession of the defendant. In many—especially civil law—jurisdictions, which is to say most of the rest of the world, there is no requirement for a party to produce information to a litigation opponent, and the plaintiff can only start an action after having marshalled virtually all of the evidence necessary to prove that the defendant committed the wrong. As a practical matter, this means that many trade secret holders with legitimate claims will not be able to file suit at all.

In designing national trade secret laws, it is therefore important for policy makers to take into account the difficulties faced by victims of trade secret misappropriation in obtaining direct proof of such misappropriation without help from the courts. One solution could be to require some form of early production of records by parties in trade secret litigation, subject to appropriate confidentiality orders. Policy makers may also wish to consider rules on burden of proof which would require the trade secret owner to present only a circumstantial case, though based on reasonable inferences, to file an action, and require the accused to present proof of independent development or discovery of the information in response to this.

The EU, as already noted, decided against securing limited recovery of information under the Enforcement Directive when it determined that trade secrets do not constitute IP rights. The opportunity remains, however, for EU member states to establish the measures described above when implementing the Trade Secrets Directive at the national level.

Protection of trade secrets during litigation

When considering the enforcement framework for trade secret disputes, policy makers are strongly urged to consider mechanisms to avoid damage to the trade secret holder's rights during the litigation process, while respecting the transparency and fairness of proceedings.

It would be ironic if litigation resulted in further damage or loss of secrets, simply because of the procedures required to resolve the dispute. But the requirement in most countries that court proceedings be open and transparent represents a serious practical impediment to filing genuine claims.

One of the most important objectives of the EU Trade Secrets Directive was to create harmonised approaches to resolving this dilemma. Courts are empowered to provide some closed proceedings and to otherwise limit access to evidence as necessary to prevent unwarranted damage to the trade secret holder's rights.

In the US, courts may limit access to confidential information to attorneys of record and approved experts. In contrast, the EU Directive requires that at least one representative of all parties have full access to all information. Courts will therefore have to exercise particular vigilance to ensure that party representatives strictly adhere to their obligations of confidentiality.

Award of damages and costs

Valuable information is usually stored and communicated digitally, making theft easy but detection difficult. Therefore, it is important that national laws provide maximum deterrence to misappropriation. This is especially important for civil cases in countries where there is no provision for punitive damages.

National governments should ensure that their laws provide for damage awards that grant full compensation to victims of trade secret theft, by including recovery not only for lost profits but also for the unfair advantage obtained by the defendant. In addition, policy makers should consider provisions like those in TRIPS Article 45, providing courts with authority to award "expenses, which may include appropriate attorney's fees". This is especially critical for SMEs who suffer trade secret loss but often lack resources to proceed against the perpetrator.

Exceptions to trade secret rights

When designing trade secret laws, policy makers may consider that other important public policy considerations justify the provision of exceptions. For example, the EU Trade Secrets Directive establishes several exceptions to liability for disclosure of trade secrets, including by whistle-blowers, in order to protect "a legitimate interest recognised by Union or national law". These exceptions were animated by a desire to protect very important interests; however, if too broadly interpreted they raise the possibility that legitimate trade secret rights may be destroyed on pretextual grounds.

Therefore, where exceptions are required or considered by national governments, they should be carefully fashioned to balance competing interests. For example, the corresponding whistle-blower provision under US law is expressly limited to communications to the authorities or a court, for the sole purpose of reporting possible criminal conduct. Exceptions for "legitimate interests" should also normally be available only as a means of tempering or limiting judicial

action by taking into account the public interest, as opposed to invocation by a private party in its own interest.

ICC hopes that this report will be helpful to both businesses and policy makers in their efforts to better protect valuable confidential business information as trade secrets. Given the increasing importance of trade secret protection for individual companies as well as for national economies and innovation as a whole, ICC hopes that policy makers around the world, drawing lessons from the EU and US approaches described in this publication, will seriously consider reviewing national legislative frameworks to ensure that they are adapted to the protection of trade secrets in light of new technological and other developments.

ABOUT THE INTERNATIONAL CHAMBER OF COMMERCE (ICC)

The International Chamber of Commerce (ICC) is the world's largest business organization with a network of over 6.5 million members in more than 130 countries. We work to promote international trade, responsible business conduct and a global approach to regulation through a unique mix of advocacy and standard setting activities—together with market-leading dispute resolution services. Our members include many of the world's largest companies, SMEs, business associations and local chambers of commerce.

We are the world business organization.

INTERNATIONAL CHAMBER OF COMMERCE

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

Publication number: 450/1081-9E
ISBN: 978-92-842-0536-3