The Computer & Internet Lawyer

Volume 34 ▲ Number 1 ▲ JANUARY 2017

Ronald L. Johnston, Arnold & Porter, LLP, Editor-in-Chief

Trade Secret Protection Measures and New Harmonized Laws

By Lothar Determann, Luisa Schmaus, and Jonathan Tam

2016 has been a big year for trade secrets in the United States and the European Union. The United States enacted the federal Defend Trade Secrets Act[1] and the European Union enacted the Directive on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.[2] Both laws have been years in the making. Both feature similarities to each other and to existing trade secret law at the state level in the United States. Neither law replaces or completely preempts existing state law. Both are intended to harmonize and enhance legal protection for business secrets and "know-how."

The US Senate noted that "[b]y improving trade secret protection, the [statute] will incentivize future innovation while protecting and encouraging the creation of American jobs." The House Report also observes that "state [trade secrets] laws vary in a number of ways and contain built-in limitations that make them not wholly effective in a national and global economy," and proclaims that the Defend Trade Secrets Act "will provide a single, national standard for trade secret misappropriation with clear rules and predictability for everyone involved."[3] Similarly, the EU states in the recitals to the EU Trade Secrets Directive that the Directive is intended to address a lack of "effective and comparable legal means for protecting trade secrets across the Union."[4]

Although only time will tell whether the new laws will achieve these legislative goals, companies should consider now how the new laws will affect their use and protection of trade secrets and how they can benefit from the legislative changes.

This article presents an overview of the Defend Trade Secrets Act and compares it to existing state trade secrets protections under the Uniform Trade Secrets Act.[5] It also explains the key features of the EU Trade Secrets Directive and compares them to the Defend Trade Secrets Act, and highlights certain features of existing German trade

Prof. Dr. Lothar Determann is a partner at Baker & McKenzie LLP in Palo Alto, CA, and teaches Computer and Data Privacy Law at the University of California, Berkeley School of Law and Hastings College of the Law and Freie Universität, Berlin. **Luisa Schmaus** is Rechtsreferendarin. **Jonathan Tam** is an associate in the technology practice group of Baker & McKenzie LLP on secondment in San Francisco and admitted to practice law in Ontario, Canada.

Wolters Kluwer

secrets law that will have to be modified pursuant to the Directive. For further comparison, the article briefly highlights the contrasting situation in Canada, a country that has not yet enacted specific trade secret law. Based on these summaries and comparisons, the article provides some practical strategic advice that global companies may wish to consider in order to protect their trade secrets and avoid infringing the rights of others under trade secrets law.

US Trade Secrets Law

The Defend Trade Secrets Act has been called a "game changer"[6] and has the potential to make a difference in litigation. However, upon closer examination, the new federal law largely codifies and harmonizes existing trade secrets law in the United States rather than changing it fundamentally. At its core, it adds a civil cause of action as well as some modifications to the existing Economic Espionage Act of 1996, which already criminalizes economic espionage and the theft of trade secrets.[7] In substance and wording, the new civil cause of action resembles existing state trade secret law and neither replaces nor preempts state law, except with respect to protections for whistleblowers that already existed under some state laws.[8]

To date, 48 states have enacted trade secrets laws on the Uniform Trade Secret Act.[9] The two hold-outs, Massachusetts and New York, have established common law trade secrets protection.[10] As noted previously, the Defend Trade Secrets Act was intended to address the variance in and jurisdictional limitations of state trade secrets law. Accordingly, the new federal law adopts many of the key elements of the Uniform Trade Secrets Act.

Trade secrets owners also may continue to bring trade secret misappropriation claims to the US International Trade Commission (ITC) under the Tariff Act of 1930.[11] The ITC is a quasi-judicial federal agency that can enjoin the import of infringing products into the United States, including articles that contain or are manufactured using misappropriated trade secrets.[12]

Definitions

The Defend Trade Secrets Act amended the definition of "trade secret" in the Economic Espionage Act to mean "all forms and types of financial, business, scientific, technical, economic, or engineering information . . . if—(A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information."[13]

This definition generally is aligned with the Uniform Trade Secrets Act[14] and requires the information at issue to (1) be secret; (2) derive independent economic value from being secret; and (3) be subject to reasonable measures to maintain its secrecy. The fact that the federal law refers to an enumerated list of information categories—whereas the California statute, for example, covers any "information"—should not make a difference in practice, given that the attribute "business" in "business information" is extremely broad. The legislative history reveals that definition in the federal law was not intended to be "meaningfully different" from the definition under state law.[15]

The Defend Trade Secrets Act did not amend the definition of trade secret "owner" in the Economic Espionage Act and thus transferred a broad criminal law definition into the realm of civil causes of action.

The Defend Trade Secrets Act did not amend the definition of trade secret "owner" in the Economic Espionage Act and thus transferred a broad criminal law definition into the realm of civil causes of action. The definition of "owner" for the purposes of the Defend Trade Secrets Act is "the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed."[16] In most other intellectual property law regimes, licensees are not entitled to bring legal actions or exclude others unless they hold an exclusive license,[17] but the Defend Trade Secrets Act does not expressly limit the group of licensees that may qualify as an "owner." The legislative history of the definition and case law under the Economic Espionage Act do not clarify this point. Because the definition of trade secret uses the singular term "the person"—as opposed to "anyone"—and based on considerations relating to actual harm, courts may nonetheless deny standing to multiple, non-exclusive licensees.

State laws vary on this point. The California Uniform Trade Secrets Act does not use or define the term "owner" in respect of a trade secret and merely states that "[a] complainant" may bring an action for misappropriation.[18] The North Carolina Trade Secrets Protection Act provides that "[t]he owner of a trade secret" may sue for misappropriation,[19] but does not define the term "owner." Under the California Uniform Trade Secrets Act, licensees have been allowed to bring actions

for trade secret misappropriation and courts have not expressly stipulated that a licensee must be an exclusive licensee.[20] A former owner of a trade secret also has been able to bring claims.[21]

Reasonable Means

What a trade secret owner is required to do to meet the "reasonable measures" requirements depends on the circumstances of each case. Most effective are actual limitations on disclosures and sharing.[22] Additionally, most US companies require employees, customers, suppliers, and other business partners to sign confidentiality agreements before they share any confidential information and implement physical, technical, and administrative safeguards to prevent unauthorized access or use.[23]

Misappropriation

Under the Defend Trade Secrets Act, a trade secret owner may bring a civil action in a federal court for trade secret misappropriation. The term "misappropriation" comprises knowingly acquiring, disclosing, or using a trade secret from an owner by improper means.[24] "Improper means" include theft, bribery, misrepresentation, espionage, and breach or inducement of a breach of a duty to maintain secrecy.[25] However, improper means does not include reverse engineering, independent derivation, or any other lawful means of acquiring the trade secret.[26] The US Supreme Court has defined reverse engineering as "starting with the known product and working backward to divine the process which aided in its development or manufacture."[27]

The California Uniform Trade Secrets Act also establishes a cause of action for the misappropriation of trade secrets. The definitions of misappropriation and improper means in the Defend Trade Secrets Act and California Uniform Trade Secrets Act are virtually identical.[28]

Remedies

The Defend Trade Secrets Act generally includes all of the remedies available under the California Uniform Trade Secrets Act, including the following:[29]

- Trade secret owners can obtain injunctions against actual or threatened misappropriation. Under the Defend Trade Secrets Act, a court may not enjoin a person from entering into an employment relationship.[30] The Uniform Trade Secrets Act does not contain such a limitation, but California courts, for example, have long rejected the "inevitable disclosure doctrine" that allows former employers in some states to enjoin employees from moving to a competitor based on a mere showing that a disclosure of trade secrets will be inevitable if the employee starts working for a competitor in a similar role.[31] California courts have rejected this doctrine because it can amount to a post-contractual non-compete covenant, which is unlawful in California.[32] In effect, Congress adopted this policy consideration with the limitation on injunctions in the Defend Trade Secrets Act.[33]

- In circumstances when completely prohibiting a party from using a misappropriated trade secret would be inequitable, a court may instead issue an injunction conditioning future use of the trade secret upon the payment of a reasonably royalty. A court also may order a party to perform specific affirmative acts to protect a trade secret. This might include destroying an article that contains a trade secret or delivering it to the trade secret owner.

- A trade secret owner whose trade secret was misappropriated may be entitled to normal damages equal to the actual loss caused by the misappropriation *and* any unjust enrichment caused by the misappropriation not addressed in computing damages for actual loss, *or*, in lieu of the above, liability for a reasonable royalty for the misappropriator's unauthorized disclosure or use of the trade secret. If the trade secret was willfully and maliciously misappropriated, the trade secret owner also may be awarded exemplary damages capped at twice the normal damages.

- Reasonable attorney fees may be awarded to a claimant in case of willful and malicious misappropriation, or to a party who prevails against a bad faith claim of misappropriation.

In "extraordinary circumstances," trade secret owners have the right under the Defend Trade Secrets Act to obtain seizure orders, that is, an order providing for the "seizure of property necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action."[34] This remedy is not expressly contained in the California Uniform Trade Secrets Act but nonetheless generally can be obtained under the broader rubric of injunctions. The Defend Trade Secrets Act prescribes a number of stringent conditions that must be met before a seizure order may be issued, such as alternative relief being inadequate and a balance of harms favoring the applicant.[35] According to the US Senate, "[t]he ex parte seizure provision is expected to be used in instances in which a defendant is seeking to flee the country or planning to disclose the trade secret to a third party immediately or

is otherwise not amenable to the enforcement of the court's orders."[36] Because information can be instantaneously replicated and transmitted electronically, any seizure order likely would need to be obtained very quickly to be effective.

Whistleblower Protection and Employer Notifications

Unlike the California Uniform Trade Secrets Act, the Defend Trade Secrets Act expressly establishes protections for whistleblowers in certain situations. The Defend Trade Secrets Act provides that an individual shall not be held criminally or civilly liable under any federal or state trade secret law for the confidential disclosure of a trade secret to a government official or attorney solely for the purpose of reporting or investigating a suspected violation of law.[37] The term "violation of law" is not defined and seems fairly broad at first sight, but it has been interpreted not to have an unlimited scope in other contexts.[38]

The Defend Trade Secrets Act provides that an individual shall not be held criminally or civilly liable under any federal or state trade secret law for the confidential disclosure of a trade secret to a government official or attorney solely for the purpose of reporting or investigating a suspected violation of law.

Unlike existing state law, the Defend Trade Secrets Act requires employers to include a notice of the whistleblower protection under the act in any agreement governing the use of a trade secret or other confidential information with an employee, contractor, or consultant. An employer that fails to provide such notice to an employee may not be awarded exemplary damages or attorney fees in an action to enforce a trade secret against such employee.[39] One scenario in which these whistleblower protection provisions could become relevant is when an employee obtains information demonstrating that the employer's product is more dangerous to the public than publicly known, and the employer takes unlawful measures to keep such information secret.[40] It already seems questionable at the outset whether the information at issue should be considered a trade secret,[41] given that the employer itself cannot derive value from the *information* per se, but merely benefits from *secrecy* by avoiding legal sanctions. Nonetheless, there is a value to the information remaining secret, which corresponds with the losses to the employer that would result from the information becoming publicly known.

US courts have not created clear general rules on whether information on corporate wrongdoings can ever be considered a trade secret.[42] Some courts have refused to enforce confidentiality agreements on public policy grounds when the unauthorized disclosures at issue related to violations of the law.[43] At the same time, courts have refused to shield a whistleblower from liability when the scope of his or her misappropriation or disclosure of confidential information was greater than that necessary to advance public policy interests.[44]

Because the Defend Trade Secrets Act only shields qualifying whistleblowers from liability under "any Federal or State trade secret law," the Act does not expressly shield them from liability under other legal theories, such as breach of contract, breach of fiduciary duty, or a violation of data privacy or security laws. The limited scope of the liability shield may not be immediately apparent to all employees, who may mistakenly believe upon reading the mandatory whistleblower protection notice that they are immune to all liability in a whistleblower situation. In practice, employers have to consider the pros and cons of providing detailed notices regarding whistleblower protection in non-disclosure agreements with employees. If they do not, they cannot claim exemplary damages or attorney fees in enforcement actions, but this possible disadvantage may be outweighed by the risk that notices confuse employees—particularly employees working abroad—and provoke a flood of illegitimate disclosures. Employers that choose to include the notice should be as clear as possible about the precise scope of the whistleblower protections afforded under the Defend Trade Secrets Act to avoid suggesting that employees are protected from liability when this is not the case.

Trade Secret Laws in Europe

Until the adoption of the EU Trade Secrets Directive earlier this year, companies in the European Union had to consider only national trade secret laws. These vary significantly from country to country, as detailed in a Baker & McKenzie study that the European Union commissioned in 2013.[45] The study found that there was no uniform definition or harmonized legal protection of trade secrets in the European Union.[46] With the EU Trade Secrets Directive, the EU Commission intends to address this lack of consistency and at the same time strengthen the protection available against the unlawful acquisition, use, or disclosure of trade secrets.[47]

EU Trade Secrets Directive

The EU Trade Secrets Directive[48] does not immediately and directly apply to companies or individuals, but requires the Member States of the European Economic Area (EEA) to transpose its rules into national law by June 9, 2018.[49] It remains up to the individual Member States how they supplement or modify national laws to meet the requirements set out in the Directive.[50] Notably, Member States are free to establish trade secrets legislation intended to be more protective than the Directive so long as they do not contradict it (*e.g.*, whistleblower immunities and permissions for reverse engineering).[51]

Definition of Trade Secret

The EU Trade Secrets Directive defines a trade secret as information that meets all of the following requirements:[52]

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

This definition is based on the definition of "undisclosed information" in the World Trade Organization's "Agreement on Trade-Related Aspects of Intellectual Property Rights" (also known as the TRIPs Agreement)[53] and contains all of the key elements of the definition of "trade secret" under the Defend Trade Secrets Act and Uniform Trade Secrets Act.

By way of comparison, to qualify as a trade secret under German national law, the information at issue must be connected to the (alleged) secret holder and subject to an economic interest, and the intent of the secret holder must be to maintain its secrecy and for it not to be easily accessible to the public.[54] Unlike the US trade secret protection regime and the EU Trade Secrets Directive, German trade secrets law does not specifically require a trade secret holder to use reasonable measures to keep the information secret. Nevertheless, such measures also are advisable under German trade secret laws: A company that does not protect its trade secrets risks them becoming easily accessible to the public or it being difficult to prove an intent and interest to maintain their secrecy.

Scope of Protection

The EU Trade Secrets Directive introduces means for trade secret holders to seek civil redress against the unlawful acquisition, use, and disclosure of trade secrets. The Directive defines a "trade secret holder" as any natural or legal person lawfully controlling a trade secret.[55] In summary, it is unlawful to acquire a trade secret by appropriating it in an unauthorized manner or by engaging in any other conduct contrary to honest commercial practices. The use or disclosure of a trade secret also is unlawful when it is carried out without the consent of the trade secret holder by a person who acquired the secret unlawfully or breaches a contractual or other duty in doing so. It also is unlawful to acquire, use, or disclose a trade secret that is known, or ought to have been known, to have been unlawfully acquired.[56]

Conversely, the acquisition of a trade secret is *lawful* when obtained by any of the following means:[57]

- Independent discovery or creation;
- Observation, study, disassembly, or testing of a product or object that has been made available to the public or that is lawfully in the possession of the acquirer of the information who is free from any legally valid duty to limit the acquisition of the trade secret;
- Exercise of the right of workers or workers' representatives to information and consultation in accordance with Union law and national laws and practices;
- Any other practice which, under the circumstances, is in conformity with honest commercial practices.

Like the Defend Trade Secrets Act, the EU Trade Secrets Directive permits developers to discover third-party trade secrets by way of reverse engineering products. Under both laws, the reverse engineering exception serves only as a defense to claims based on trade secrets law and not, for example, claims under copyright law for reproducing and adapting in the process of reverse engineering computer programs.[58]

By contrast, current German law does not permit the acquisition of someone else's trade secret through reverse engineering if it involves a significant expenditure of time and resources.[59] For example, the Munich Higher Regional Court decided that reverse engineering a gaming machine is unlawful when the machine's mode of operation only can be discovered by using 70 hours of observation and € 2,500 of gaming money.[60] The body of German case law exploring the permissible limits of reverse engineering is limited. This may

be because German judicial procedures lack a discovery process and prosecuting a party for unlawful reverse engineering is challenging without the ability to compel relevant evidence. Germany will have to change its national trade secret law in this respect based on the EU Trade Secrets Directive.

Remedies

Details regarding remedies and procedural rules under the EU Trade Secrets Directive differ from those under the Defend Trade Secrets Act. This is not surprising, given the different civil procedure systems on both sides of the Atlantic and even within the European Union. Nonetheless, the basics are similar.

First, the EU Trade Secrets Directive establishes remedies directed at prohibiting the production, offering, use, importation, exportation, and placing on the market of "infringing goods", which are defined to mean "goods, the design, characteristics, functioning, production process or marketing of which significantly benefits from trade secrets unlawfully acquired, used or disclosed."[61] This definition encompasses not only products containing a trade secret (*e.g.*, an electronic toy containing a copy of confidential computer software), but also products that were made using secret processes (*e.g.*, a knife manufactured using a confidential steel welding process). The Defend Trade Secrets Act is less specific in this respect, but US courts and the ITC have discretion to issue injunctions that capture both types of products.

Second, the EU Trade Secrets Directive establishes that judicial authorities may order the dissemination of information about an infringer's unlawful acquisition, use, or disclosure of a trade secret at the expense of the infringer.[62] The Defend Trade Secrets Act does not expressly contemplate this possibility, but unlike in most EU Member States, US courts regularly publish their judgments and other decisions with names of the parties and trade secret owners are free to tout their victories in press releases or even in advertisements, if they choose.

In addition to these two remedies that are not expressly contained in the Defend Trade Secrets Act, the EU Trade Secrets Directive lists a number of remedies that also appear in the US law:

- Injunctions, including against the unlawful use or disclosure of a trade secret and the production, offering, use, or circulation of infringing goods.[63]

- An order to perform corrective measures, including recalling infringing goods from the market, depriving the infringing goods of their infringing quality, destroying infringing goods, seizing or delivering up suspected infringing goods, and destroying or delivering up any object which contains or embodies the trade secret.[64]

- In circumstances when an injunction or an order to perform corrective measures would be inappropriate, pecuniary compensation based on the royalties or fees that would have been due had that person requested authorization to use the trade secret in question for the relevant period of time.[65]

- Damages to be quantified in consideration of all appropriate factors, which may include the negative economic consequences suffered by the injured party, any unfair profits made by the infringer and "the moral prejudice" caused to the injured party.[66] The reference to moral prejudice suggests that judicial authorities may have the option to award damages in excess of the injured party's actual economic loss. As with the Defend Trade Secrets Act, damages pursuant to the EU Trade Secrets Directive also may be based on the amount of royalties or fees that would have been due had the infringer requested authorization to use the trade secret in question.[67]

The EU Trade Secrets Directive does not include any provisions concerning the award of legal costs. How legal costs are awarded in a private dispute varies across EEA Member States. However, many EEA jurisdictions have a "loser pays" rule that entitles the prevailing party to attorney fees.[68] Similarly, the Defend Trade Secrets Act contemplates such a rule as an exception to the general rule in US litigation where each party usually has to bear its own costs.

The EU Trade Secrets Directive does not provide for criminal penalties, although it does not preclude Member States from retaining or enacting such provisions. In Germany, violations of existing trade secret law may result in fines or up to five years imprisonment in extraordinary circumstances. Unless the German legislature repeals this provision, it will survive the transposition of the EU Trade Secrets Directive into German law.

Whistleblower Protection and Other Exemptions

Like the Defend Trade Secrets Act, the EU Trade Secrets Directive aims to protect whistleblowers in certain situations.[69] In particular, the measures, procedures, and remedies under the directive must be "dismissed where the alleged acquisition, use or disclosure of the trade secret was carried out … for revealing misconduct, wrongdoing or illegal activity, provided that the respondent acted for the purpose of protecting the general public interest."[70]

On its face, this protection is broader than those under the Defend Trade Secrets Act, which only protects disclosures (1) in confidence; (2) to a government official or attorney; and (3) solely for the purpose of reporting or investigating a suspected violation of law.[71] In contrast, the whistleblower protection under the EU Trade Secrets Directive seemingly extends to any disclosure (not necessarily one made in confidence) that relates to any misconduct or wrongdoing (and not solely suspected violations of the law) to any person or entity (not just government officials and attorneys) if the purpose (but not necessarily the only purpose) of the disclosure is to protect the general public interest. In several respects, the protection under the EU Trade Secrets Directive is materially more expansive than that afforded by the Defend Trade Secrets Act.

The whistleblower protection under the EU Trade Secrets Directive seemingly extends to any disclosure (not necessarily one made in confidence) that relates to any misconduct or wrongdoing (and not solely suspected violations of the law) to any person or entity (not just government officials and attorneys) if the purpose (but not necessarily the only purpose) of the disclosure is to protect the general public interest.

Besides the exception for whistleblowers, the EU Trade Secrets Directive includes another remarkable defense not found in the Defend Trade Secrets Act or existing trade secret laws in US states, namely "for exercising the right to freedom of expression and information as set out in the [Charter of Fundamental Rights of the European Union[72] (the Charter)], including respect for the freedom and pluralism of the media."[73] By way of background, Article 11 of the Charter provides as follows: "(1) Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. (2) The freedom and pluralism of the media shall be respected."[74]

In the past, the European Court of Human Rights invoked Article 11 of the Charter to protect whistleblowers, citing the public interest in the disclosed information.[75] Yet, because the EU Trade Secrets Directive now expressly protects whistleblowers separately, the "freedom of expression" defense logically must be intended to cover other scenarios. If the whistleblower defense was not meant to create a specific and separate defense that at the same time precludes the application of the freedom of expression defense as a *lex specialis*, then this could seriously undermine trade secret protection in the EU/EEA. If this was not the case, then this could lead to employees and others starting to disclose trade secrets indiscriminately in the hope of support from constitutional and human rights courts that could counteract the European Union's attempt to create reliable criteria for business and know-how protection.

In the United States, clashes between trade secret law and free speech rights granted by the First Amendment have been rare, even though the United States protects free speech more profoundly than probably any other country in the world.[76] Citizens are protected only against state actors under the civil rights amendments to the US Constitution and courts apply restrictions on speech based on trade secret laws in an opinion-neutral manner, which does not warrant strict or even intermediate scrutiny under the First Amendment doctrine. For example, in *DVD Copy Control Assn., Inc. v. Bunner*, the California Supreme Court affirmed that trade secrets constitute a kind of property and the First Amendment does not prohibit courts from incidentally enjoining speech to protect a legitimate property right.[77]

Trade Secrets in Canada

Not all advanced economies and legal systems have opted for specific trade secret legislation. Canada, for example, does not have any comprehensive provincial or federal civil trade secret statute comparable to the Defend Trade Secrets Act or EU Trade Secrets Directive. Although the Uniform Law Conference of Canada adopted a Uniform Trade Secrets Act in 1989 (with different text from the one adopted by the US Uniform Law Commission),[78] it has not been enacted into law by any provincial or federal legislature.

Canada, however, has enacted the Security of Information Act which, similar to the US Economic Espionage Act, criminalizes economic espionage. Economic espionage includes the misappropriation, alteration, or destruction of a trade secret for the benefit of a foreign economic entity and to the detriment of Canada's economic, diplomatic, or security interests. A "trade secret" is defined in the statute as any information that:[79]

- Is or may be used in a trade or business;
- Is not generally known in that trade or business;

- Has economic value from not being generally known; and

- Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

This definition incorporates all of the main concepts found in the definitions under the Defend Trade Secrets Act and EU Trade Secrets Directive.

Without a comprehensive civil trade secrets statute, the protection of trade secrets has been left to case law. Canadian courts have applied general laws protecting confidences and confidential information to what would constitute trade secrets in the United States or under the new EU Directive. The Supreme Court of Canada affirmed the following elements of a breach of confidence action in 1989, which have since been applied consistently by Canadian courts:[80]

- The information at issue must not be available to the public;

- The information must have been communicated in circumstances imparting an obligation of confidence on the recipient; and

- There must be unauthorized use of that information to the detriment of the party that first communicated it.

There is no explicit requirement under Canadian law for information to be subject to "reasonable measures" to keep it secret for it to qualify for protection under Canadian trade secret law.[81] This diverges from the definition of trade secret in the Canadian Security of Information Act, as well as that in the US Defend Trade Secrets Act and EU Trade Secrets Directive. Canadian courts nevertheless consider whether the trade secret at issue was known to the trade or the public[82] and there is an implied connection to the "reasonable measures" concept in that a trade secret would often be known to the trade or the public if it were valuable and not subject to reasonable measures to keep it secret.

Canadian law characterizes breach of confidence as a *sui generis* action founded on the principles of contract, equity, and property. This is at least partly so that courts have the flexibility to issue a broad range of remedies to address perceived injustices arising from a breach of confidence.[83] Remedies available for trade secret misappropriation under Canadian law therefore include legal and equitable remedies such as compensatory damages, punitive damages, an accounting for profits earned from the breach, injunctions, the seizure of property containing trade secrets, and constructive trusts.[84]

A comprehensive Canadian trade secrets statute similar to the laws in the United States and European Union would likely help to codify and harmonize Canadian trade secrets case law and provide greater certainty to trade secret owners, parties engaging in reverse engineering, employees unsure of their confidentiality obligations, potential whistleblowers, and other relevant stakeholders.

Global Strategies and Practical Measures to Protect Trade Secrets

As in many other areas of law and business, companies are confronted with different national laws in various jurisdictions as they expand globally. Multinationals typically will want to use key know-how information globally throughout their business, regardless of what law may apply in a particular country. However, if they become entangled in a dispute, a local court will apply local law to the question of whether the company is entitled to protection of its trade secrets or liable for misappropriation of another company's trade secrets. Today, a company must show reasonable means to maintain secrecy in support of claims in a US court—but not necessarily in Canada or Germany. It is permitted to reverse engineer a competitor's products to determine its trade secrets in the United States, but not (yet) in Germany. It may prevent a former employee from joining a competitor in some US states based on the inevitable disclosure doctrine, but not in California, not under the Defend Trade Secrets Act, and not under German law. Whistleblowers also can be treated quite differently in different jurisdictions under existing trade secret laws.

As already discussed, the new Defend Trade Secrets Act and the EU Trade Secret Directive will bring some harmonization to the rules applicable to whistleblowers, reverse engineering, reasonable means requirements, and other aspects of trade secrets law. Still, neither law will provide full harmonization because neither completely preempts or replaces existing trade secret laws in its respective jurisdiction. Further, both laws are limited in their territorial application and will not apply in countries outside their jurisdiction. Consequently, companies should continue to carefully analyze applicable trade secret rules in different jurisdictions, particularly in the context of development programs and disputes with whistleblowers.

Yet, with respect to different positions on "reasonable means" requirements in different jurisdictions' trade secret laws, companies find a much easier answer to the question of what they should do in light of

different laws: Apply the highest standard worldwide. First of all, companies need to apply reasonable protection means because that is the most effective way to actually—not just legally—protect their trade secrets. Second, applying protection means as such does not create any disadvantages in any jurisdiction; aside from resource considerations and a need to localize contractual protections, there is no real trade-off decision to make. Third, companies have to implement data security measures anyhow in more and more jurisdictions to protect personal data under data privacy laws, which pursue different goals but prescribe similar technical and organizational measures.[85] Fourth, various new cybersecurity rules, requirements, and initiatives require or encourage companies to take measures to protect their information.

Minimization

Companies should implement protocols and procedures to minimize the unnecessary reproduction and sharing of trade secrets within their organization. Every disclosure, every new person with access, every additional copy means additional risks for secrecy. Nevertheless, the need for secrecy must be balanced against the need to foster cooperation and transparency within the organization and partner networks that make up the extended enterprise.

In virtually any circumstance that involves sharing a trade secret with another party, a reasonable and effective means of maintaining the secrecy of a trade secret is to enter into a confidentiality agreement with that party.

Confidentiality Agreements

In virtually any circumstance that involves sharing a trade secret with another party, a reasonable and effective means of maintaining the secrecy of a trade secret is to enter into a confidentiality agreement with that party. Because different types of relationships contemplate different types of disclosures, companies should avoid using a standard confidentiality agreement for every third party with whom they share confidential information. In particular, they should consider the following key issues when drafting a confidentiality agreement appropriate to their situation:

- **Scope and Definition of Confidential Information.** Depending on whether the company shares or receives more secrets in a particular relationship, they could define "confidential information" more strictly (*e.g.*, by requiring markings or including only certain types of information) or broadly (*e.g.*, to cover any information, unless it is public, or include all information that a reasonable person in like circumstances would consider confidential).

- **Prohibited and Permitted Disclosures.** Depending on interests, companies can provide for one-sided or mutual disclosure restrictions or qualify mutuality with tactical exceptions and definitions.

- **Use Restrictions.** Companies should clearly state the purposes for information sharing (*e.g.*, evaluation of licensing opportunity, M&A due diligence) and strictly prohibit any other use of the data (*e.g.*, development of competing product after licensing or acquisition negotiations fail).

- **Security Measures.** Prescribing specific security measures (*e.g.*, adherence to an international security standard) that a party receiving confidential information must implement can establish how the parties expect such information to be protected. Related to these obligations might be a general duty to observe a minimum degree of care when protecting confidential information, such as the use of "best", "reasonable", or "commercially reasonable" efforts to protect such information.

- **Assignments.** In many mergers, acquisitions, and corporate reorganizations, business information is transferred with employees and assets. Yet, such information is usually covered by non-disclosure agreements that do not expressly permit assignments. To avoid unrealistic and overly burdensome restrictions, companies should consider expressly addressing limited assignability in certain non-disclosure agreements.

- **Governing Law and Venue.** Including a contractual choice of law clause is good practice to avoid uncertainty. A venue clause, on the other hand, is usually not helpful, given that the trade secret owner may need to seek preliminary injunctive relief at short notice wherever a threat emerges and injunctions are usually not enforceable across borders, not even within the United States.[86] If companies have a good idea where they may need to enforce, they also should consider translations or bilingual versions that will afford better access to local courts.

- **Term and Termination.** Confidentiality obligations usually should survive termination of a business relationship for a reasonable time period or indefinitely.

- **Notice regarding Whistleblower Immunities.** US employers have to weigh the relative benefits of including versus omitting whistleblower notices as required by the Defend Trade Secrets Act.

When you draft a confidentiality agreement, consider also translation requirements and public policy limitations on restrictive covenants, for example, on post-contractual non-compete clauses, employee invention assignments, and other covenants. Also, consider whether you can conveniently cover in the same agreement loosely related objectives or requirements, for example, obtaining licenses to information or satisfying obligations to impose data secrecy commitments under data protection laws.

If you review a confidentiality agreement, look out for potentially problematic add-on terms, such as representations or warranties regarding information accuracy, ownership or non-infringement, licenses, assignment clauses, etc. Also, it can be worth considering whether what you need is really a "non-confidentiality agreement," that is, an agreement that clarifies that you do not have to protect information that you receive, for example, in the context of unsolicited proposals.

Physical, Technical, and Organizational Measures

Minimization and confidentiality agreements tend to be the two most important measures, but they are not the only ones to maintain the secrecy of trade secrets. You also may wish to consider implementing the following measures to protect trade secrets:[87]

- **Physical, technical, and organizational safeguards.** Companies should implement appropriate physical, technical, and organizational security safeguards to protect trade secrets from unauthorized access, use, disclosure, loss, and modification. Physical safeguards include physical barriers, lock-and-key mechanisms, and paper shredders. Organizational safeguards include well-designed and enforced policies and protocols, and regular training around confidentiality obligations. Technical safeguards include passwords, firewalls, automated intrusion detection systems, and authentication measures. The safeguards companies choose to implement should be tailored to the specific activities of their organization.

- **Recruitment, hiring, training, and termination.** In most companies, employees are the most important source of trade secret development. However, they also present one of the most significant risks to trade secrets. Entry and exit interviews, frequent training, and monitoring are crucial.

- **Confidentiality notices.** Companies should appropriately mark materials containing confidential information and trade secrets (*e.g.*, by way of watermark or a heading) to indicate their confidential nature. In cases when different types of confidential information are subject to different levels of protection, the notices can inform parties of the proper level of protection intended to be extended to the information. At the same time, whether information constitutes confidential information subject to confidentiality obligations should generally not be conditioned exclusively on whether a confidentiality notice has been affixed to it. Otherwise, the confidentiality obligations would not apply to information communicated orally or in situations when one forgot to apply a confidentiality notice or the notice was inadvertently modified or removed. It also is important not to apply confidentiality notices to materials that can be disclosed publicly without any issue—otherwise, they may be taken less seriously by parties.

Trade Secrets Inventory

A trade secrets inventory can be an essential document for establishing a company's ownership of, and rights and interests in, the trade secrets listed in the inventory. It also can help to ensure that your company's trade secrets are properly protected and that your company is able to demonstrate to relevant stakeholders that this is the case. Preparing such a list of trade secrets also may result in additional business benefits such as facilitating the discovery of underutilized trade secrets.

The trade secrets inventory should list the trade secrets or types of trade secrets owned by your company and identify the jurisdictions in which they are stored and used so that it is clear which legal regimes apply to which trade secrets. Of course, in the interest of secrecy, the list should not describe the information in such detail that it could result in creating additional security risks. Other important information that should be included in the inventory are: (1) whether a trade secret is owned or licensed; (2) who has access to which trade secrets; (3) what measures are used to protect each trade secret; (4) how much each trade secret is worth; and (5) when a trade secret is expected to expire (if ever), for example if it is expected to form the basis of a patent

application. It also may be worth it to create categories of trade secrets, ranging from low, medium, and highest level of importance.

The trade secrets inventory can be used to determine whether there are any gaps in your company's trade secret protection and what steps it can take to address such gaps or otherwise strengthen such protection. The inventory should be updated regularly to ensure that your company's assessment of what trade secrets it owns and how well they are protected remains current and accurate.

Misappropriation Action Plan

Companies also should prepare for inevitable security breaches, that is, situations involving a real and present threat of misappropriation by unlawful acquisition, use, or disclosure of a trade secret. Preparedness is crucial because in a threat situation you must act quickly to prevent irreparable harm and imminent dissemination and qualify for preliminary injunctions and other temporary remedies.

In "dry run exercises" and when developing your breach response plan, you should determine the steps that the company should take to: (1) terminate or limit access to your trade secrets; (2) investigate and document the details of a breach; and (3) seek remedies in response to the breach. In your action plan, you should identify who is responsible for taking which steps; executing a successful misappropriation action plan likely requires a multi-disciplinary approach that involves the participation of information technology personnel, directors, lawyers, records managers, and public relations staff, as necessary.

Specific steps to be taken will differ depending on the circumstances of the breach, including the nature of the breach (intentional or accidental), type of data affected (personal data, trade secrets, confidential information owned by third parties, etc.), the identity of actual or potential infringers (business partners under contract, employees, criminals, state actors, etc.), jurisdictions affected, and phase of misappropriation (*i.e.*, whether the trade secret is only exposed to potential acquisition, or already acquired, used, disseminated, etc.).

A separate but related action plan should be developed to address special considerations relating to requirements under data privacy laws, because these regimes are different from trade secrets and other IP regimes. After an action plan has been developed, it is important to ensure the action plan is readily accessible to individuals with responsibilities thereunder, implement training to facilitate the execution of the action plan, and update it regularly according to all relevant legal and business considerations.

In conclusion, although global trade secret laws will not be completely harmonized any time soon, businesses can safeguard their interests through careful housekeeping and planning.

Notes

1. Defend Trade Secrets Act, 114 P.L. 114-153, available at *https://www.congress.gov/bill/114th-congress/senate-bill/1890/text*, codified, as amended, 18 U.S.C. §§ 1831-1836 and 1838-1839 [Defend Trade Secrets Act].
2. Council Directive (EC) 2013/0402, available at *http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:PE_76_2015_INIT&from=EN*.
3. H. Rept. 114-529.
4. EU Trade Secrets Directive, Recitals 4-10.
5. Implemented in California in Cal. Civ. Code §§ 3426-3426.11.
6. David Snyder and David Almeling, Trade Secret Law and Corporate Strategy § 2.08 (2015).
7. 18 U.S.C. §§ 1831-1839; *see* "Stealing Trade Secrets and Economic Espionage: An Overview of the Economic Espionage Act," Charles Doyle, *Congressional Research Service*, August 19, 2016, available at *http://www.fas.org/sgp/crs/secrecy/R42681.pdf*.
8. 18 U.S.C. § 1838.
9. Published by the Uniform Law Commission in 1979 and amended in 1985, available at *http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf*.
10. *Intellectual Property and Antitrust Law*, William C. Holmes, 2016 Thomson Reuters, Rel. 59 3/2016, § 2:2, 2-19 and § 2:4, 2-40.
11. Tariff Act of 1930, Codified at 19 U.S.C. ch. 4 [Tariff Act].
12. 19 U.S.C. § 1337, *see*, *e.g.*, TianRui Group Co. v. ITC, 661 F.3d 1322, 2011 U.S. App. LEXIS 20607, 100 U.S.P.Q.2D (BNA) 1401, 33 *Int'l Trade Rep.* (BNA) 1385 (Fed. Cir. 2011). For more information, *see* Jeffrey Kessler and Spencer Waller, *International Trade and U.S. Antitrust Law*, Second Edition, 2006: Thomson/West, at § 13:6.
13. 18 U.S.C. § 1839(3).
14. *See*, *e.g.*, Cal. Civ. Code § 3426.4(d): "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (1) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and (2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.
15. H. Rept. 114-529 ("While other minor differences between the UTSA and Federal definition of a trade secret remain, the Committee does not intend for the definition of a trade secret to be meaningfully different from the scope of that definition as understood by courts in States that have adopted the UTSA.").
16. *Id.*, § 1839(4).
17. *See*, Lothar Determann, "Taking IPR Burdens with Tax Benefits—Non-exclusive intra-group licensing can adversely

affect recovery in infringement actions against third parties," 74 BNA's *Patent, Trademark & Copyright Journal* 1836 (2007).

18. *Id*., § 4326.3; Uniform Trade Secrets Act § 3.
19. N.C. Gen. Stat. § 66-153.
20. Ajaxo Inc. v. E*Trade Group Inc., 135 Cal. App. 4th 21, 26 (Cal. App. 6th Dist. 2005).
21. Jasmine Networks, Inc. v. Super., Ct., 180 Cal. App. 4th 980, 986 (Cal. Ct. App. 2009).
22. As Benjamin Franklin observed, "Three may keep a secret, if two of them are dead." Benjamin Franklin, *Poor Richard's Almanack*, The U.S.C. Publishing Co. Waterloo, Iowa, 1914, 53.
23. For more practical suggestions, *see* the section of this article entitled "Global Strategies and Practical Measures to Protect Trade Secrets."
24. 18 U.S.C. § 1839(5).
25. *Id*., § 1839(6)(A).
26. *Id*., § 1839(6)(B).
27. Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476, 94 S. Ct. 1879, 40 L. Ed. 2d 315, 181 U.S.P.Q. (BNA) 673 (1984).
28. H. Rept. 114-529 ("The [Defend Trade Secrets Act] bill … models its definition of "misappropriation" on the Uniform Trade Secrets Act."). Examples of differences include that the California Uniform Trade Secrets Act uses the verb "utilize" (Cal. Civ. Code § 3426.1(b)(2)(B)(i)) whereas the Defend Trade Secrets Act uses the verb "use" in the same context (18 U.S.C. § 1839(5)(B)(ii)(I)). Cal. Civ. Code § 3426.1(a) provides that "reverse engineering or independent derivation alone shall not be considered improper means."
29. 18 U.S.C. § 1836(b)(3); Cal. Civ. Code §§ 3426.2-3426.4.
30. 18 U.S.C. § 1836(b)(3)(A)(i)(I).
31. PepsiCo, Inc. v. Redmond, 54 F.3d 1262, 1269 (7th Cir. 1995) ("A plaintiff may prove a claim of trade secret misappropriation by demonstrating that [the] defendant's new employment will inevitably lead him to rely on the plaintiff's trade secrets").
32. *See*, *e.g.*, Bayer Corp. v. Roche Molecular Sys., Inc., 72 F. Supp. 2d 1111, 1120 (N.D. Cal. 1999) ("To the extent that the theory of inevitable disclosure creates a de facto covenant not to compete without a nontrivial showing of actual or threatened use or disclosure, it is inconsistent with California policy and case law.")
33. H. Rept. 114-529 ("These limitations on injunctive relief were included to protect employee mobility, as some have expressed concern that the injunctive relief authorized under the bill could override State-law limitations that safeguard employee mobility and thus could be a substantial departure from existing law in those states.")
34. 18 U.S.C. § 1836(b)(2)(A)(i).
35. *Id*., §§ 1836(b)(2)(A)(ii)(I)–1836(b)(2)(A)(ii)(VIII).
36. S. Rept. 114-220.
37. 18 U.S.C. § 1833(b).
38. For example, Cal. Civ. Code § 1668 voids any contract intended to exempt anyone from responsibility for a "violation of law." However, California courts have not let any tort suffice. For example, in Delta Air Lines, Inc. v. McDonnell Douglas Corp., 503 F.2d 239, 1974 U.S. App. LEXIS 6277 (5th Cir. Ga. 1974), the US Court of Appeals for the Fifth Circuit held that contracts limiting liability for negligence do not fall afoul of this provision.
39. 18 U.S.C. § 1833(b).
40. An analogy might be drawn to the disclosures made by Jeffrey Wigand from 1994 to 1996 regarding the harmful effects of certain tobacco products in contravention of confidentiality agreements that he had signed. *See* Carol M. Bast, "At What Price Silence: Are Confidentiality Agreements Enforceable?," *William Mitchell Law Review*, Vol. 25: Iss. 2, Article 14, at 628 (1999).
41. *See* Christoph Schnabel, Rechtswidrige Praktiken als Betriebs- und Geschäftsgeheimnisse?, CR 2016, 342 ff.
42. As S. Rept. 114-220 states, "[t]he available literature suggests that few [trade secret claims] have been brought against [whistleblowers] under current law." Nevertheless, *see* Walsh v. Amerisource Bergen Corp., 2014 U.S. Dist. LEXIS 82064, 2014 WL 2738215 (E.D. Pa. June 16, 2014), in which a relator under the False Claims Act, 31 U.S.C.S. §§ 3729–3733, appropriated vendor agreements, customer contracts, documents containing pricing, credit transactions, and sales analysis information, customer lists and customer information, audit reports, and documents pertaining to the defendants' standard operating procedures. These documents were held to constitute trade secrets.
43. For example, in Lachman v. Sperry-Sun Well Surveying Co., 457 F.2d 850, a contractor for an oil and gas company breached a non-disclosure agreement by informing a third party that the oil and gas company was drawing oil from the third party's property. The court held that public policy prohibited the enforcement of the non-disclosure provision against the contractor because the oil and gas company's misappropriation of the third party's oil and gas was tortious. *See also* United States v. Cancer Treatment Ctrs. of Am., 350 F. Supp. 2d 765, 2004 U.S. Dist. LEXIS 22974, 22 *I.E.*R. Cas. (BNA) 202 (N.D. Ill. 2004).
44. *See*, *e.g.*, Cafasso v. Gen. Dynamics C4 Sys., 637 F.3d 1047, 2011 U.S. App. LEXIS 5979, 31 *I.E.*R. Cas. (BNA) 1802 (9th Cir. Ariz. 2011). In this case, a relator under the False Claims Act appropriated almost 11 gigabytes of materials—often without reviewing their contents—purportedly for the purposes of bringing an action against her employer under the False Claims Act. The US Court of Appeals for the Ninth Circuit described her appropriation of the materials as vast and indiscriminate and affirmed the district court's finding against her for breaching her confidentiality agreement.
45. "Study on trade secrets and confidential business information in the internal market," *http://ec.europa.eu/DocsRoom/documents/14900* and *http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_final-study_en.pdf*; summary at *http://ec.europa.eu/DocsRoom/documents/14900* and *http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_appendix-18_en.pdf*.

46. Opinion of the European Economic and Social Committee on the Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, COM(2013) 813 final–2013/0402 (COD) (Opinion on EU Trade Secrets Directive).
47. EU Trade Secrets Directive, Recital 8 ("The differences in the legal protection of trade secrets provided for by the Member States imply that trade secrets do not enjoy an equivalent level of protection throughout the Union, thus leading to fragmentation of the internal market in this area and a weakening of the overall deterrent effect of the relevant rules.") and Recital 10 ("It is appropriate to provide for rules at Union level to approximate the laws of the Member States so as to ensure that there is a sufficient and consistent level of civil redress in the internal market in the event of unlawful acquisition, use or disclosure of a trade secret.").
48. *See* Lorenzo de Martinis, Rembert Niebel, and Birgit Clark, "The new EU Trade Secrets Directive: all change to trade secret protection in Europe?," *Journal of Intellectual Property Law & Practise*, to be published early 2017 on the EU Trade Secret Directive and current trade secret protection in Europe.
49. *Id.*, Article 19(1). The EEA consists of the 28 EU Member States plus Iceland, Liechtenstein, and Norway.
50. *See* Mathias Lejeune, Die neue EU Richtlinie zum Schutz von Know-How und Geschäftsgeheimnissen, CR 2016, 330.
51. EU Trade Secrets Directive, Recital 10 ("Those rules should be without prejudice to the possibility for Member States of providing for more far-reaching protection against the unlawful acquisition, use or disclosure of trade secrets, as long as the safeguards explicitly provided for in this Directive for protecting the interests of other parties are respected.").
52. *Id.*, Article 2(1).
53. Annex 1C of the Marrakesh Agreement Establishing the World Trade Organization, signed in Marrakesh, Morocco on April 15, 1994, article 39, available at *https://www.wto.org/english/tratop_e/trips_e/t_agm3d_e.htm*#7; *see also* Opinion on EU Trade Secrets Directive, *supra* n. 46 at paragraph 1.7.
54. Ohly/Sosnitza/Ohly, UWG, 7th Ed. (2016), § 17 Rn. 5.
55. EU Trade Secrets Directive, Article 2.
56. *Id.*, Article 4.
57. *Id.*, Article 3 no. 1.
58. Copyright laws in the EU and in the United States provide for separate and different defenses relating to reverse engineering under certain conditions, *e.g.*, intermediate copying to determine functional elements of interfaces to achieve interoperability with independently developed computer programs. *See* Lothar Determann and David Nimmer, "Software Copyright's Oracle from the Cloud," 30 *Berkeley Tech. L. J.* 161, 175-176 and 180-181 (2015).
59. *RGZ* 149, 329, 334–"*Stiefeleisenpresse"*; *BGH*, GRUR 1980, 750; *BGH* GRUR 2008, 727; *Reimann*, GRUR 1998, 298; *OLG Munich*, GRUR 1991, 694; *Erbs/Kohlhaas*, Strafrechtliche Nebengesetze, 208. EL Mai 2016, § 17 UWG para 10 et seq; *Ohly/Sosnitza*, UWG, 7th ed., § 17 UWG para 10.
60. *OLG Munich*, GRUR 1991, 694.
61. EU Trade Secrets Directive, Articles 2(4), 10 and 12.
62. *Id.*, Article 15.
63. *Id.*, Article 12(1).
64. *Id.*, Article 12.
65. *Id.*, Article 13. Judicial authorities are required to take into account a number of factors when considering an application for an injunction or corrective measures order, including the measures taken to protect the trade secret, the conduct of the infringer, and the legitimate interests of the parties. Pecuniary compensation may be ordered instead of an injunction or corrective measures at the infringer's request where certain prescribed conditions are met.
66. *Id.*, Article 14(2).
67. *Id.*
68. Study on the Transparency of Costs of Civil Judicial Proceedings in the European Union, commissioned by the European Commission, Contract JLS/2006/C4/007-30-CE-0097604/00-36, December 2016, available at *https://e-justice.europa.eu/fileDownload.do?id=99bdd781-aa3d-49ed-b9ee-beb7eb04e3ce.*
69. EU Trade Secrets Directive, Recital 20 ("The measures, procedures and remedies provided for in this Directive should not restrict whistleblowing activity.").
70. *Id.*, Article 5(b).
71. 18 U.S.C. § 1833(b)(1).
72. 2012/C 326/02.
73. EU Trade Secrets Directive, Article 5(b).
74. "EU Charter of Fundamental Rights," European Commission, last updated August 2, 2016, available at *http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm.*
75. *See*, *e.g.*, Heinsich v. Germany, European Court of Human Rights Judgment dated 21.07.2011-28274/08, at para. 60.
76. Lothar Determann, Kommunikationsfreiheit im Internet–Freiheitsrechte und gesetzliche Beschränkungen [Freedom of Communications on the Internet–Civil Rights and Statutory Limitations], Baden Baden (1999); Internet Freedom and Computer Abuse, 35 *Hastings Communications & Entertainment Law Journal* 429 (2013).
77. DVD Copy Control Assn., Inc. v. Bunner, 31 Cal. 4th 864, at 881 (Cal. 2003). *But see* Pamela Samuelson, "Principles for Resolving Conflicts Between Trade Secrets and the First Amendment," UC Berkeley Public Law Research Paper No. 925056 (August 9, 2006), available at SSRN: *http://ssrn.com/abstract=925056.*
78. Uniform Trade Secrets Act (1989), Uniform Law Conference of Canada, available at *http://www.ulcc.ca/en/home/537-josetta-1-en-gb/uniform-actsa/trade-secrets-act/730-uniform-trade-secrets-act-1989.*
79. Security of Information Act, RSC 1985, c O-5, s. 19.
80. Lac Minerals Ltd. v. International Corona Resources Ltd., [1989] SCJ No 83. *See also Halsbury's Laws of Canada*

(Online), Patents, Trade Secrets, and Industrial Designs (Hughes, Clarizio), (II.1(2)) at HPT-183.

81. Section 4.7 of *Sookman: Computer, Internet and Electronic Commerce Law (Online)* appears to cite only United States and other international cases for the proposition that "[r]easonable measures to protect information in confidence, not perfection, is generally required" under Canadian trade secrets law (last accessed September 16, 2016).

82. Lac Minerals Ltd v. International Corona Resources Ltd, at para. 55; Reliable Toy Co v Collins, [1950] OJ No 126, at para. 67.

83. Cadbury Schweppes Inc. v. FBI Foods Ltd., [[1999] 1 SCR 142 (Supreme Court of Canada), at para. 28, per Binnie J. ("The sui generis concept was adopted to recognize the flexibility that has been shown by courts in the past to uphold confidentiality and in crafting remedies for its protection."). *See also* Apotex Fermentation Inc v. Novopharm Ltd, [1998] MJ No 297 (Manitoba Court of Appeal), at paras. 111-113.

84. *Sookman: Computer, Internet and Electronic Commerce Law (Online)*, section 4.9 (last accessed September 16, 2016). *See also Halsbury's Laws of Canada (Online),* Patents, Trade Secrets, and Industrial Designs (Hughes, Clarizio), (II.4(2)) at HPT-192; *see also* Mortil v. International Phasor Telecom Ltd, [1988] BCJ No 249 (British Columbia County Court) for an example of a seizure order issued in respect of a computer program incorporating a trade secret.

85. *See* Lothar Determann, Determann's *Field Guide to Data Privacy Law*, 2nd Ed. (2015), p. 122; Lothar Determann and Jesse Hwang, "Data Security Requirements Evolve: From Reasonableness to Specifics," 26 *Computer & Internet Lawyer* Issue 9, p. 6 (2009).

86. *See* Lothar Determann and Saralyn Ang-Olson, "Recognition and Enforcement of Foreign Injunctions in the United States—Yahoo!, Inc. v. La Ligue contre Le Racisme et L'Antisemitisme—influential precedent for the freedom of speech on the Internet or routine confirmation of long established principles regarding equitable relief?", *Computer Law Review International* 2002, 12; *Corporate Counsel's International Advisor*, August 1, 2004.

87. *See also Trade Secret Law and Corporate Strategy*, Darin W. Snyder and David S. Almeling, LexisNexis, 2015 edition.