ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Preparing for Life Under the New US and European Trade Secret Laws

Compliance and Ethics

Intellectual Property


the PATENT PROCESS

CHEAT SHEET

- ***Security in secrets.*** The signing of the Defend Trade Secrets Act imposes a uniform standard that allows businesses to plan their trade secret strategies with confidence that they will have a remedy in the event of misappropriation.
- ***The EUTSD.*** The European Union Trade Secrets Directive was created shortly after the DTSA and similarly protects against the misuse of trade secrets, clarifying a description of unlawful disclosure and threatening heavy injunctions.
- ***Is this misappropriation?*** The DTSA forbids the acquisition of a trade secret by "improper means," as well as the disclosure of a trade secret by someone who knew that it was a trade secret.
- ***Whistleblower protections.*** Whistleblowers are granted immunity by the DTSA holding that they disclose trade secrets in confidence to federal, state, or local officials in attempt to report a suspected violation of law.

Within the span of a few weeks, both the United States and the European Union instituted sweeping new changes to their trade secret laws. In the United States, President Barack Obama's signing of the Defend Trade Secrets Act (or DTSA) on May 19, 2016 elevated trade secrets to equal status with traditional forms of intellectual property protections: patent, copyright, and trademark. For the first time, companies will be able to bring civil suits under federal law to remedy trade secret misappropriation, with the right to both damages and injunctions. The European Union's Trade Secrets Directive (or EUTSD) was adopted by the EU Council on May 27, 2016, and will be implemented over the next two years by member states (which, of course, may not include the United Kingdom). The directive begins the process of bringing uniformity to the European market's trade secret standards.

The new laws should be welcome news for in-house counsel and senior management. Informational assets have become the foundation for many businesses' value, and maintaining secrecy has become a primary strategy for protecting them. The change was driven in part by the slow weakening of traditional intellectual property protections. In the United States, for example, it has become difficult to patent many software and business method innovations that previously had been given legal protection. The slow pace of the patent system also means that many inventions have become obsolete by the time a patent is issued. Gaining a patent requires publicly disclosing the innovation — something many companies may simply be unwilling to do for their most important technologies.

The DTSA recognizes that the use of secrecy to protect prized developments has become the new norm. The legislation supplements a hodgepodge of state laws that resulted in inconsistent protections and procedural requirements. The new law not only opens the federal courts to trade secret owners, expanding the scope of discovery and reach of enforcement; it also establishes important new remedies, including damages and injunctions. In emergency situations where trade secret materials may be destroyed or removed from the county (and therefore potentially beyond the scope of enforcement), the DTSA allows trade secret owners to seek an ex parte seizure. Most importantly, the new law imposes a uniform standard that will apply nationwide, allowing businesses to plan their trade secret strategies with the assurance that they will have a remedy in the event of misappropriation.

The threat to business is real. The FBI estimates that American businesses alone suffer more than US$13 billion in trade secrets losses every year. Though corporations often focus on the very real threat from data security breaches, trade secrets are most commonly lost when employees move to a competitor or to start up their own business. Trade secret disputes are also increasing between proposed partners who share information under non-disclosure agreements (NDAs). The situation often arises when a smaller, newer company makes broad disclosure of technical and business information to a strategic investor, joint development partner, or potential acquirer. When the proposed transaction falls through, both sides face risk. The disclosing company may find that their information or knowhow is used by the acquiring company, but must then demonstrate that improper use, a challenge when the disclosures are not carefully documented and controlled. Conversely, even innocent companies who acquire confidential information under NDAs may find themselves confronted with litigation by disappointed counterparties, and then must demonstrate that their technology was developed independently, free of contamination by information disclosed in negotiations.

The risk of loss and litigation is not limited to businesses in high technology, life sciences, and other fields heavily reliant on research and development. As detailed below, trade secrets encompass a wide variety of information that would be valuable to competitors and derives its value from being

confidential. That includes commercial information like pricing sheets, business strategy, or customer lists. Financial services and sales-intensive businesses often face dire consequences from the loss of confidential business information.

At the same time that in-house lawyers will want to put in place the necessary measures to ensure that their informational assets enjoy legal protection, they will also want to avoid the threat of litigation. Proper procedures for on-boarding new employees, for managing and monitoring the conduct of dispersed sales staff, and for controlling information obtained during the course of negotiating potential business partnerships are all critical for ensuring that costly litigation does not cripple operations.

Of course, as all in-house lawyers know, what makes for sound legal policy may not find a receptive audience with management, who often view compliance as a hindrance to operations. But the implementation of the new laws may provide a good opportunity not just for legal teams to take stock of their trade secret programs, but to push for the changes needed to ensure that businesses are protected.

What business assets are protected as “trade secrets”?

The DTSA and EUTSD protect information that is kept confidential and derives economic value from that confidentiality. This encompasses a broad swath of commercially useful information. Importantly, neither require that the information be novel, unlike patent law or other intellectual property regimes.

What is “confidential”?

The DTSA is an amendment to the Economic Espionage Act, which created criminal liability for trade secret misappropriation but did not provide a private civil cause of action. Under the predecessor statute, a criminal action could be brought for misappropriation of information that was not generally available to “the public.” That definition created some ambiguity, especially with respect to information that was known to industry experts but would not be known to the public at large.

After some debate, Congress adopted a definition of trade secrets that more closely parallels the Uniform Trade Secrets Act, the model statute that has been enacted by many states. Under the DTSA, the test for confidentiality is now whether the information is generally known or readily ascertainable by *“another person who can obtain economic value from the disclosure or use of the information”* — a definition that most commonly applies to a competitor. Notably, the DTSA does not preempt state law, so existing protections remain available in appropriate circumstances.

Under the EUTSD, protected information is that which *“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.”* This language arguably encompasses a smaller range of information than the DTSA, although in practice the difference may be minimal. It is important to keep in mind that the precise scope of terms such as “generally known” and “readily accessible” will likely need to be interpreted in the coming years, potentially even by the Court of Justice of the European Union.

What measures must be taken to protect secrecy?

The DTSA offers protection for information only if a trade secret owner *“has taken reasonable*

measures to keep such information secret." That definition does not impose rigid requirements for what security will be deemed adequate, but trade secret owners must be prepared to show that they took adequate steps to protect the confidentiality of their information. The "reasonable measures" standard requires businesses to protect their confidential information in proportion to its value, the feasibility of security measures, and industry standards. At a minimum, businesses should ensure that they inform employees of what information is deemed confidential and of their obligation to protect it, implement physical and data security restrictions (such as including "confidential" legends), limit access to required personnel, and ensure proper exit procedures for departing personnel. Legal documents, including employment agreements and NDAs, should be reviewed carefully.

The EUTSD requires that a trade secret be *"subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret."* Again, the EUTSD provides little guidance on what "reasonable steps" might entail. Such steps may include restricting access to the information and using NDAs. As with the scope of protectable information, there is a strong possibility that this will be interpreted by European courts in the coming years.

What constitutes misappropriation?

Both the DTSA and EUTSD protect against what is essentially the misuse of trade secrets by others. The DTSA authorizes a civil action in United States federal court for misappropriation of a trade secret where the secret is *"related to a product or service used in, or intended for use in, interstate or foreign commerce."* "Misappropriation" is defined* in a lengthy manner that resembles the Uniform Trade Secrets Act. In sum, the DTSA forbids the acquisition of a trade secret by "improper means," as well as use or disclosure of a trade secret by someone who knew that it was a trade secret or otherwise owed a duty to the owner of the trade secret.

* "[T]he term 'misappropriation' means — (A) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or (B) disclosure or use of a trade secret of another without express or implied consent by a person who — (i) used improper means to acquire knowledge of the trade secret; (ii) at the time of disclosure or use, knew or had reason to know that the knowledge of the trade secret was — (I) derived from or through a person who had used improper means to acquire the trade secret; (II) acquired under circumstances giving rise to a duty to maintain the secrecy of the trade secret or limit the use of the trade secret; or (III) derived from or through a person who owed a duty to the person seeking relief to maintain the secrecy of the trade secret or limit the use of the trade secret; or (iii) before a material change of the position of the person, knew or had reason to know that — (I) the trade secret was a trade secret; and (II) knowledge of the trade secret had been acquired by accident or mistake . . ."

Importantly, "improper means" is defined in an open-ended manner as *"includ[ing] theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means."* This means that confidentiality and NDAs may provide an important "hook" for trade secret owners to bring assets under the protection of the DTSA's regime. However, reverse engineering and "independent discovery" are expressly excluded from the definition of "improper means."

The EUTSD takes a slightly different approach from the DTSA by setting forth circumstances under which acquisition, use, or disclosure of a trade secret is "unlawful." Unlawful acquisition is:

- Unauthorized access to, appropriation of, or copying of any documents, objects, materials,

substances, or electronic files, lawfully under the control of the trade secret holder, containing the trade secret or from which the trade secret can be deduced;
- Any other conduct which, under the circumstances, is considered contrary to honest commercial practices[.]

Building on that description, the EUTSD describes unlawful use or disclosure as:

- Having acquired the trade secret unlawfully;
- Being in breach of a confidentiality agreement or any other duty not to disclose the trade secret;
- Being in breach of a contractual or any other duty to limit the use of the trade secret[.]

UNDER THE DTSA AND EUTSD, POTENTIALLY PROTECTABLE TRADE SECRETS INCLUDE:

- Source code
- Customer lists
- Pricing, sales, and marketing strategies
- Manufacturing processes
- Recipes
- Profit margins

Importantly, another provision of the EUTSD extends unlawful use to include *"offering or placing on the market of infringing goods"* when *"the person carrying out such activities knew, or ought, under the circumstances, to have known that the trade secret was used unlawfully."* This may prove to be a powerful tool for businesses to pursue end-sellers of goods manufactured by infringing manufacturers. Like the DTSA, the EUTSD expressly immunizes "independent discovery or creation" and reverse engineering.*

* Described as "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."

As a general matter, the EUTSD is once again arguably narrower in some ways than the DTSA, as it specifies three forms of "unlawful use or disclosure." In contrast, the DTSA adopts an openended definition of what activities constitute "improper means." However, the EUTSD's attempt to govern downstream sellers may provide new reach to trade secret owners and new risks to businesses that sell potentially infringing goods. Once more, European courts will likely be called upon to provide guidance over competing interpretations of terms such as "honest commercial practices."

DTSA and Economic Espionage Act

All forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing

if:

- the owner thereof has taken reasonable measures to keep such information secret; and,
- 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.

UTSA

Information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

- derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and,
- is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

EUTSD

- 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;
- has commercial value because it is secret;
- has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

What remedies are available under the DTSA and EUTSD?

The DTSA's default remedy is an injunction against actual or threatened misappropriation, as well as damages for actual losses and unjust enrichment. Reasonable royalties may also be available under certain circumstances. However, the DTSA also includes a novel seizure procedure that authorizes *ex parte "seizure of property necessary to prevent the propagation or dissemination"* of allegedly misappropriated trade secrets. Although it is available only "in extreme circumstances," and is subject to other stringent limitations, this procedure may provide powerful leverage for trade secret owners.

The EUTSD similarly authorizes a broad swath of remedies, including provisional and permanent injunctions, seizure of infringing goods, and payment of compensation, measurable as damages, lost profits, or royalties, to a rights-holder.

Businesses should take steps now to prepare, including the following:

1. Identify and categorize trade secrets and add "confidential" legends or markings on all related documents associated with the trade secrets.
2. Ensure protective measures sufficient to establish entitlement to trade secret status, and are documented to permit quick enforcement action.

3. Review and improve every link of manufacturing or production chains to ensure “reasonable” secrecy measures are in place at each link.
4. Review and improve physical security protections.
5. Review and improve protections for electronic data security.
6. Balance security with practical needs of business while maintaining legally protected status.
7. Review employment agreements (including contractor and consultant agreements), in particular for potential notice requirements imposed by the new laws.
8. Review and improve NDA management.
9. Initiate training and reinforcements.
10. Ensure strong exit processing for departing employees with an emphasis on affirming continuing confidentiality obligations as set forth in any related proprietary information and inventions agreement (PIIA) signed as a condition of their prior employment.
11. Review procedures and legal agreements used for collaborations where confidential information is shared or created.
12. Ensure scrutiny during new employee hiring and on-boarding process, particularly emphasizing that no third party trade secrets or confidential information is brought or disclosed to your organization.
13. Understand whistleblower and other “legal disclosure” risks.
14. Prepare a plan for quick response in case a problem arises.

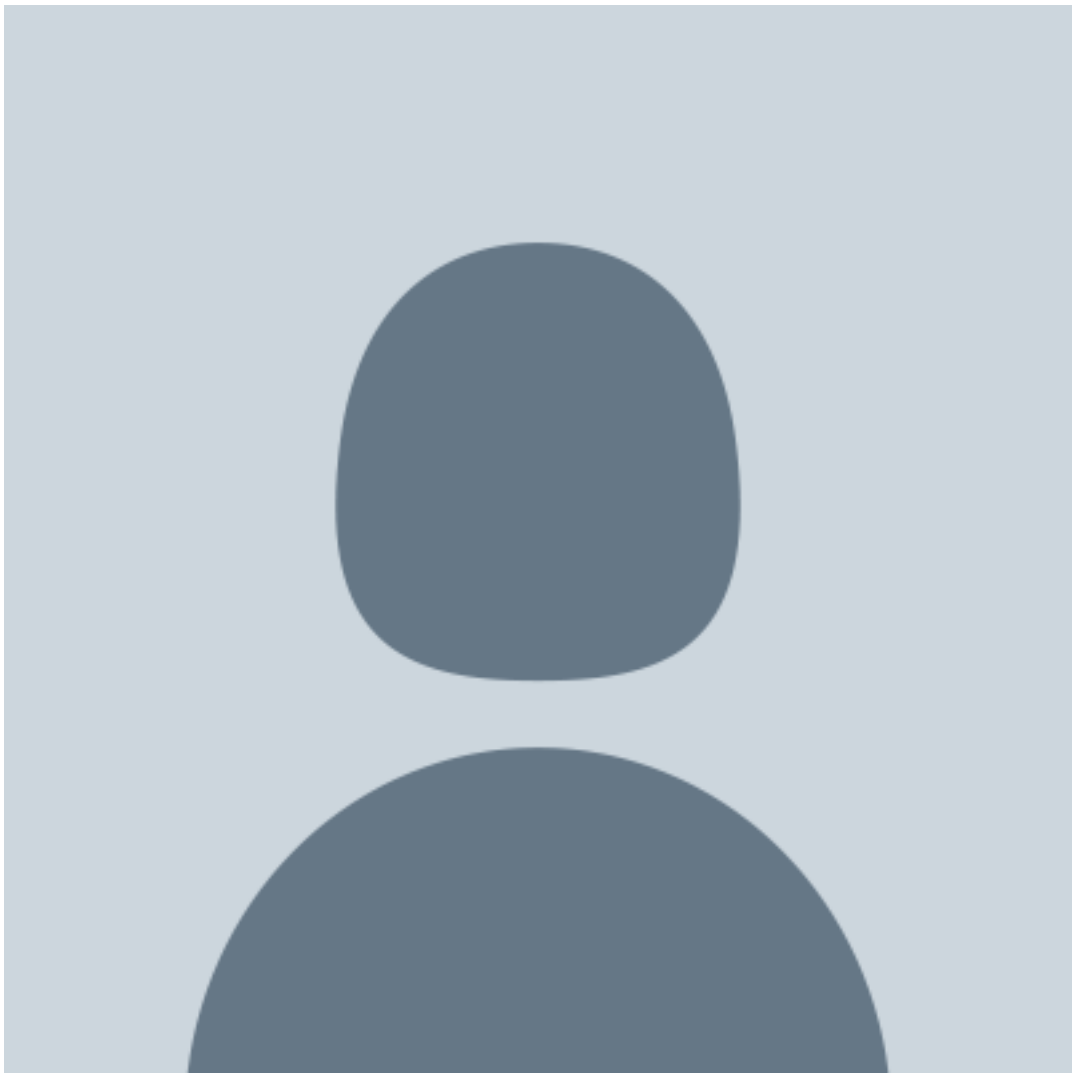
What protections are available for whistleblowers?

The DTSA provides for immunity to whistleblowers. Specifically, it mandates that no liability — whether criminal or civil, or under federal or state law — will be imposed for disclosing a trade secret *“in confidence to a Federal, State, or local government official, either directly or indirectly, or to an attorney . . . solely for the purpose of reporting or investigating a suspected violation of law”* or in a *“complaint or other document filed in a lawsuit”* so long as the filing is made under seal. The DTSA further contains an anti-retaliation provision that immunizes disclosure in a *“lawsuit for retaliation by an employer for reporting a suspected violation of law”* so long as documents disclosing the secret are filed under seal and the employee does not otherwise improperly disclose the secret.

In order for an employer to obtain exemplary damages and attorney’s fees in an action against an employee, the DTSA requires that “employees” be provided notice in any *“contract or agreement . . . that governs the use of a trade secret or other confidential information.”* Importantly, “employees” includes contractors and consultants. This provision applies to contracts and agreements “entered into or updated” after the DTSA’s enactment on May 11, 2016.

The EUTSD expressly mandates that its provisions *“should not restrict whistleblowing activity”* and *“should not extend to cases in which disclosure of a trade secret serves the public interest, insofar as directly relevant misconduct, wrongdoing or illegal activity is revealed.”* Notably, the EUTSD expressly permits (although does not require) member states to allow this exception to encompass good faith belief by a potential whistleblower that the requirements of the EUTSD had been met. “[M]isconduct, wrongdoing or illegal activity” under the EUTSD may encompass a greater range of activities than the DTSA’s “suspected violation of law;” however, as with the provisions discussed above, there is a strong possibility that judicial guidance will be needed in the coming years.

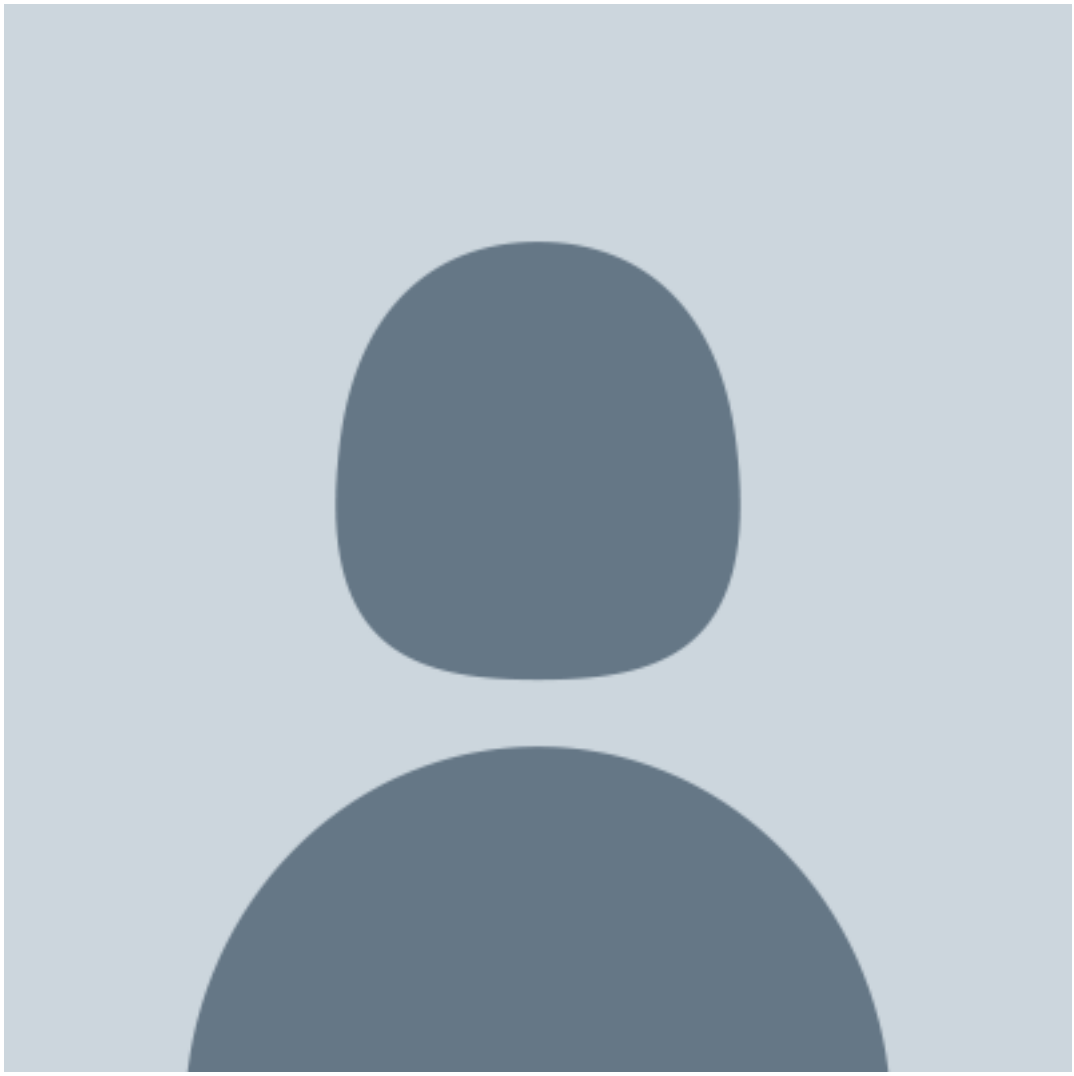
Robert Finnell



Calypso Technology, Inc.

Robert Finnell has served as senior vice president, general counsel, and corporate secretary for Calypso Technology, Inc., a global application software provider for the capital markets industry, financial institutions, and other companies participating in the world’s financial markets.

Michael K. Ng



San Francisco-based trial lawyer

Kobre & Kim

Michael K. Ng is a San Francisco-based trial lawyer who leads the intellectual property and technology litigation group at Kobre & Kim, a conflict-free international law firm focused exclusively on disputes and investigations.