

**ITechLaw 2015 European Conference**  
Intellectual Property Interactive Workshop  
Paris, France, October 17, 2014  
Facilitator Robert Milligan, Seyfarth Shaw LLP<sup>1</sup>

*Trade Secret Protections and Legislative Developments in the United States and EU*

Trade secrets and proprietary information are an often overlooked form of intellectual property in some countries or not considered intellectual property in others. Nevertheless, many companies derive tremendous value from such information, and litigation often ensues when misappropriation or breach occurs. Proposed legislation in the United States and a proposed Directive in Europe seek to increase trade secret protections and the uniformity of trade secrets laws. This IP workshop will discuss the proposed legislation, the various interests involved, and the pros and cons of such legislation, its chances of success, and it will facilitate a lively discussion of the basic principles any legislation should contain.

**I. How Are Trade Secrets Currently Protected in the United States?**

In the United States, trade secrets consist of information and can include a formula, pattern, compilation, program, device, method, technique or process. To meet the most common definition of a trade secret, it must be used in business, and give an opportunity to obtain an economic advantage over competitors who do not know or use it. Trade secrets are generally protected by statute under the Uniform Trade Secrets Act (UTSA). The UTSA, published by the Uniform Law Commission (ULC) in 1979 and amended in 1985, was an act promulgated in an effort to provide a unified legal framework to protect trade secrets.

Texas recently became the 48th state to enact some version of the UTSA. New York and Massachusetts are the remaining states not to have enacted the UTSA. Trade secrets are protected in those jurisdictions under the common law.

Trade secrets are also protected under federal criminal laws, i.e. the Economic Espionage Act of 1996, as well as state criminal laws.

Unlike patent, trademark, or copyright protection, there is no set time period for trade secret protection. A trade secret is protected as long as it is kept secret. However, once a trade secret is lost, it is lost forever. As we have seen in a post-WikiLeaks world, once confidential information is disclosed, it can be instantly distributed online for hundreds of millions to see, access, and download, and thereby lose its trade secret status.

---

<sup>1</sup> Seyfarth Shaw attorneys Dan Hart (Atlanta), Joshua Salinas (Los Angeles) Razia Begnum (London) and Andrew J. Masak (Atlanta) assisted with the preparation of these materials. For updates on the U.S. legislation and Directive as it proceeds through the legislative process, please refer to Seyfarth Shaw's "Trading Secrets" blog at [www.tradesecretslaw.com](http://www.tradesecretslaw.com).

## A. What Is the Proposed U.S. Legislation?

The proposed legislation would authorize a private civil action in federal court for the misappropriation of trade secrets when certain circumstances are present and certain specified requirements are met. Two bills have been recently introduced into Congressional committee:

### 1. Senate Bill: Defend Trade Secrets Act

On April 29, 2014, Sens. Christopher Coons (D-Del.) and Orrin Hatch (R-Utah) introduced the [Defend Trade Secrets Act of 2014](#). The bill amends the [Economic Espionage Act](#) to provide a civil cause of action to private litigants for violations of 18 U.S.C. § 1831(a) and 1832(a) of the EEA and for “misappropriation of a trade secret that is related to a product or service used in, or intended for use in, interstate or foreign commerce.” According to the Senate sponsors, the bill will provide uniform trade secrets protection and federal remedies across the United States.

The bill marked the latest attempt in the past four years to create a private civil cause of action for trade secret misappropriation at the federal level. The following bills previously failed: Amendment to Currency Exchange Rate Oversight Reform Act of 2011, Protecting Trade Secrets and Innovation Act of 2012 (“PATSI”), and the Private Right of Action Against Theft of Trade Secrets Act of 2013 (“PRATSA”).

The bill uses the statutory language for “improper means” and “misappropriation” from the UTSA. The bill also provides for a five year statute of limitations and provides uniform remedies for misappropriation of trade secrets. It provides for injunctive relief to prevent any actual or threatened misappropriation of trade secrets. It also allows for affirmative actions to be taken to protect trade secrets, such as protective orders. With respect to damages, it provides damages for actual loss, unjust enrichment, and a reasonable royalty in certain scenarios. Additionally, in exceptional circumstances, royalties can be awarded for the use of trade secrets in lieu of a permanent injunction. In cases of willful or malicious misappropriation, the bill provides for exemplary damages of not more than three times the actual damages. It also provides for attorneys fees’ and costs for willful and malicious misappropriation or for the pursuit of a trade secret cause of action in bad faith.

It also provides for *ex parte* orders for preservation of evidence and seizure of any property used, in any manner or part, to commit or facilitate a violation of the statute, using the procedure contained in the Lanham Act.

Lastly, the bill provides that nothing in the statute “shall be construed . . . to preempt any other provisions of law.” Accordingly, the intent of the bill is not to preempt state UTSA claims.

### 2. House Bill: Trade Secrets Protection Act

On July 29, 2014, a similar bill, entitled the [Trade Secrets Protection Act of 2014](#), was introduced into the House, by a bi-partisan group led by George Holding (R-N.C.) and Jerrold Nadler (D-NY).

“American businesses face relentless cybersecurity threats every day, costing our economy billions of dollars and tens of thousands of jobs each year,” said Rep. George Holding in his [press release](#) in support of the bill.

“As a way to help create jobs, grow our economy and protect our businesses, I have introduced the Trade Secrets Protection Act of 2014. This bill will help supply American businesses, both large and small, with the tools needed to combat these destructive threats,” he added.

“American businesses are global leaders in innovation and job creation, yet they are faced with increasing threats to valuable information. The current patchwork within state and federal statutes is not enough to keep pace with organized trade secret theft, resulting in a loss of nearly \$100 billion which could mean 200,000 jobs, a recent report stated,” he remarked.

“By helping American businesses defend against these threats, we are not only protecting American interests, but helping recover the millions of dollars and thousands of jobs lost each year,” Holding concluded.

The bill was originally co-sponsored by Holding, Howard Coble, R-N.C., Hakeem Jeffries, D-N.Y., Steve Chabot, R-Ohio and John Conyers, D-Mich. Additional House members have subsequently joined these members in co-sponsoring the bill.

### **3. What Are The Differences Between The Two Bills?**

The House bill largely tracks the Senate’s Defend Trade Secrets Act but has three notable and significant modifications:

1. It only permits a civil claim for “misappropriation of a trade secrets that is related to a product or service use in, or intended for use in, interstate or foreign commerce.” It does not permit a claim for a violation of 18 U.S.C. § 1831(a) and 1832(a).
2. It permits a seizure order on an *ex parte* basis to preserve evidence or to prevent the propagation or dissemination of the trade secret that is the subject of the action but it has certain precautions and limitations not found in the Senate bill.
3. It clarifies that it only covers misappropriation actions that occur on or after it is enacted.

With respect to the seizure order language, in order to obtain an *ex parte* order, the plaintiff must show, that (1) a temporary restraining order under Federal Rule of Civil Procedure 65(b) would be inadequate because the defendant would evade, avoid, or otherwise not comply with such order; (2) an immediate and irreparable injury will occur if seizure is not ordered; (3) the harm to the plaintiff of denying the order outweighs the legitimate interests of defendant and substantially outweighs any harm to third parties; (4) the plaintiff is likely to succeed against the defendant in showing that the defendant misappropriated the trade secret and is in possession of the trade secret; (5) the plaintiff described with particularity the matter to be seized and the location where the matter is to be seized; (6) the defendant would destroy or make the property inaccessible to the court if the applicant were to proceed on notice; and (7) the plaintiff has not publicized the request.

Additionally, the court's order must (1) minimize any interruption of the business operations of third parties and the defendant that is unrelated to the trade secret that has allegedly been misappropriated; (2) protect the property from disclosure to plaintiff; (3) set a hearing date no later than seven days after the order is issued; and (4) require a security adequate to cover damages from a wrongful or excessive seizure. The court is required to take appropriate action to protect the defendant from publicity. The court is also required to take custody of the material ordered seized. Lastly, any person who suffers damage by reason of a wrongful or excessive seizure has a cause of action against the plaintiff.

Accordingly, the House bill provides even more restrictions and safeguards on the ability to obtain an *ex parte* seizure order. In sum, the most significant difference between the bills is the clarification and refinement of the seizure order and the exclusion of section 1831 and 1832 civil claims.

## **B. Do We Need Federal Trade Secrets Legislation?**

Many business, professional, political, and academic leaders have called for the creation of federal civil cause of action for trade secret misappropriation. There has been some vocal opposition to the legislation.

Recent scholarly articles in the *Gonzaga Law Review* and *Fordham Law Review* indicate that federal courts may be more equipped to devote resources to trade secret claims so as to establish a uniform body of case law, like other intellectual property. See *A Statistical Analysis of Trade Secret Litigation in State Courts*, 46 *Gonzaga Law Review* 57 (February 2011); *Four Reasons to Enact a Federal Trade Secrets Act*, 19 *Fordham Intellectual Property, Media & Entertainment Law Journal* 769 (April 2009).

Additionally, published reports indicate that there is a growing rise in trade secret theft from foreign hackers and rogue employees interested in obtaining U.S. businesses' trade secrets. Foreign economic collection and industrial espionage against the United States represent significant and growing threats to the nation's prosperity and security. In response, the Obama Administration released a [150-page report](#) that unveiled a government-wide strategy designed to reduce trade secret theft by hackers, employees, and companies. In its published strategy plan, the Obama Administration recognized the accelerating pace of economic espionage and trade secret theft against U.S. corporations and suggested looking into creating additional legislative protections.

Additionally, security company Mandiant published a [report](#) finding that the Chinese government is sponsoring cyber-espionage to attack top U.S. companies. Moreover, CREATE.org released a [whitepaper](#) that highlighted how far-reaching and deeply challenging trade secret theft is for companies operating on a global scale. Further, a [report](#) commissioned by IT security company Symantec revealed that half of the survey respondents, employees from various countries, including the United States, revealed that they have taken their former employer's trade secret information, and 40 percent say they will use it in their new jobs. Lastly, estimates of trade secret theft range from one to three percent of the Gross Domestic Product of

the United States and other advanced industrial economies, according to a new [report](#) by PwC US and CREATE.org.

Indeed, the [recent expansion of penalties](#) and [expanded definition of trade secrets](#) under the EEA reflects a recognition by the government that the EEA is a valuable tool to protect secret, valuable commercial information from theft and that Congress can work in a bi-partisan effort to address such theft.

The significant harm caused by economic espionage for the benefit of foreign actors is illustrated by a recent case where a project engineer for the Ford Motor Company copied 4,000 Ford Motor Company documents onto an external hard drive and delivered them to a Ford competitor in China. The documents contained trade secret design specifications for engines and electric power supply systems estimated to be worth between \$50 million and \$100 million. Similarly, a former employee of a North American automotive company and the employee's spouse were found guilty of stealing trade secrets related to hybrid vehicle technology worth \$40 million. The couple intended to sell the information to a Chinese competitor.

There is also significant harm caused by economic espionage committed by insiders. An employee of a large U.S. futures exchange company pleaded guilty to stealing more than 10,000 files containing source code for a proprietary electronic trading platform. Prosecutors estimated the value of these trade secrets between \$50 and \$100 million. The employee said he and two business partners had planned to use this source code to develop their own company.

The United States currently has an un-harmonized patchwork of trade secret protection laws that are ill-equipped to provide an effective civil remedy for companies whose trade secrets are stolen. Not all states have adopted the Uniform Trade Secrets Act, and many differ in the interpretation and implementation of certain trade secret laws. For instance, states have differences in their definition of a trade secret (e.g. Idaho expressly includes computer programs) and what is required to maintain a claim for trade secret misappropriation. Some states have found a novelty requirement for information to be considered a trade secret and some are more protective of customer lists. There are also several states that have different statute of limitations for trade secret claims and there are also significant differences on the availability of a royalty injunction. Many states also did not pass Section 8 of the UTSA which provides, “[t]his [Act] shall be applied and construed to effectuate its general purpose to make uniform the law with respect to the subject of this [Act] among states enacting it.” Moreover, victims of trade secret theft can face lengthy and costly procedural obstacles in obtaining evidence when the misappropriators flee to other states or countries or transfer the evidence to other states or countries.

### **C. Proponents and Sponsors of the Bills**

The two pending trade secret bills have bi-partisan support in both houses by high ranking legislators. Additionally, the [Heritage Foundation](#) recently wrote an [article](#) in support of a private right of action. Congresswoman Zoe Lofgren, D-Cal., previously proposed creating a civil cause of action in federal court last year with the [PRATSA bill](#). Also, a diverse set of companies and organizations have [come out in favor of legislation or the concept of a federal civil cause of](#)

[action](#), including Adobe, Boeing, Microsoft, IBM, Honda, DuPont, Eli Lilly, Broadcom, Caterpillar, NIKE, Qualcomm, General Electric, Michelin, 3M, United Technologies Corporation, AIPLA, IPO, National Association of Manufacturers, and the National Chamber of Commerce.

As indicated NAM supports the bill, noting that it marked “a critical step toward ensuring manufacturers can effectively and efficiently enforce their trade secrets at home and abroad.” “[Trade secret] theft costs businesses in this country some \$250 billion a year,” the group said. “The Trade Secrets Protection Act would help to address this challenge by providing access to federal civil enforcement for trade secrets theft. Right now, businesses must go state by state to defend their rights.”

Proponents of the bills have cited the advantages of a federal cause of action, as among other things, a unified and harmonized body of law that addresses discrepancies under the existing law and provides companies a uniform standard for protecting its proprietary information. Federal legislation will treat trade secrets on the same level as other IP and establish them as a national priority, address national security concerns, and create a demonstrative effect on major foreign jurisdictions. The bill may also provide a complimentary measure to combat trade secret misappropriation by private industry in light of strained government resources. A federal cause action may also provide service of process advantages, the ease of conducting nationwide discovery, and additional remedies to aid victims, such as seizure.

Additionally, the former head of the [Patent Office](#), David Kappos recently came out in favor of the bill on behalf of the Partnership of American Innovation stating, “Trade secrets are an increasingly important form of intellectual property, yet they are the only form of IP rights for which the protection of a federal private right of action is not available. The Trade Secrets Protection Act will address this void, and the PAI supports its swift enactment.”

Erik Telford of the [Franklin Center for Government and Public Integrity](#) added, “[t]he weakness of these laws is that there is no overarching legal framework at the federal level to account for both the sophistication and international nature of new threats. As Mr. Kappos noted, even the government is bound by finite resources in its efforts to protect companies, evidenced by the fact that under the Economic Espionage Act, the Department of Justice initiated only 25 cases of trade secret theft last year.”

#### **D. Opposition To The Bills**

A group of 31 professors from throughout the United States who teach and write about intellectual property law, trade secret law, invocation and/or information have submitted an [Opposition Letter](#) to the two bills. The professors cite five primary reasons for their opposition: (1) effective and uniform state law already exists; (2) the proposed Acts will damage trade secret law and jurisprudence by weakening uniformity while simultaneously creating parallel, redundant, and/or damaging law; (3) the Acts are imbalanced and could be used for anti-competitive purposes; (4) the Acts increase the risk of accidental disclosure of trade secrets; and (5) the Acts have potential ancillary negative impacts on access to information, collaboration among businesses, and mobility of labor. A [forthcoming article](#) by Washington and Lee

University School of Law professor Christopher Seaman critiques the federalization of trade secrets law. See also Mr. Seaman's [related guest post](#) at the Patently-O blog.

## **E. Current Status Of Proposed Legislation**

Both bills have been introduced into their corresponding judiciary committee.

The Senate Judiciary Committee held a [closed-door briefing on September 4, 2014](#) to review the proposed legislation.

In the House, the bill was [reported favorably to the full House](#) after a House Judiciary Committee markup hearing on September 17, 2014.

The House may vote on the bill before the end of 2014 in the lame duck session following the early November elections. It remains to be seen whether the Senate will consider the bill prior to end of 2014.

## **II. Highlights of Proposed European Commission Directive for Trade Secrets Protection**

On November 28, 2013, the European Commission announced a proposal for a Directive on trade secrets.<sup>2</sup> If passed by the European Parliament, the Directive will increase the trade secrets protections afforded to companies with operations in the EU and may greatly enhance cross-border certainty and uniformity across Europe.

At this stage in the legislative process, the Directive remains merely a proposal. However, several aspects of the Directive, if adopted, would substantially alter the existing legal landscape and create a more harmonized trade secret regime throughout the EU.

Three features of the Directive are particularly noteworthy.

First, the Directive provides a common definition of "trade secrets" and uniform rules about the acquisition, use, and disclosure of trade secrets. For example, in language that is similar to the definition of "trade secrets" in the Uniform Trade Secrets Act (which the vast majority of U.S. states have adopted), the proposed Directive defines a trade secret as "information which meets all the following requirements":

- "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 a secret"; and

---

<sup>2</sup> See 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 (available at <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52013PC0813>)



- “has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.”

The proposed Directive also provides that acquisition of a trade secret is unlawful “whenever carried out intentionally or with gross negligence by”:

- unauthorized access to or copy 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;
- theft;
- bribery;
- deception;
- breach or inducement to breach a confidentiality agreement or any other duty to maintain secrecy; or
- any other conduct which, under the circumstances, is considered contrary to honest commercial practices.

Second, the Directive establishes a common set of procedures and remedies for trade secret holders where there is unlawful acquisition, use, or disclosure of that trade secret, including a two-year statute of limitations for bringing claims for trade secret misappropriation.<sup>3</sup> The Directive also includes rules on the preservation of trade secrets during litigation.

Third, the Directive provides for uniform remedies for civil law redress for trade secrets misappropriation across Member States, including injunctive and declaratory relief, damages, and sanctions for non-compliance. The Directive also includes various reporting provisions.

It is unclear whether the Directive as currently written will be implemented, if at all. If the Directive does come into force, Member States will still need to implement the Directive within two years from the date of adoption of the Directive into their own national law. EU directives lay down certain end results that must be achieved in every Member State by a specific date. Individual Member States must adapt their laws to meet these goals, but are free to decide how to do so.

The EU Council issued its position on the directive in the spring of 2014. In general, the Council supports the Directive with some minor changes: a) the Council proposes a six-year limitation period on suing over trade secrets compared to the two years proposed by the Commission; b) the Council’s version clarifies that national laws may provide greater protection for trade secrets than that set out in the directive; and c) and the Commission’s draft required a trade secret holder to show that an alleged infringer had acted ‘intentionally’ or with ‘gross negligence’ and the

---

<sup>3</sup> As noted below, following the European Commission’s introduction of the proposal, the Council of the European Union has issued its position on the directive and has suggested some revisions to the proposal, including lengthening the statute of limitations to 6 years.



Council has removed this requirement. The Council has also requested changes to allow the restricted disclosures of trade secrets during and after trade secret litigation which are broader than permitted in the Commission's proposal.

The draft directive is currently being reviewed by the EU Parliament's Legal Affairs, Internal Market, and Industry Committees and their decisions have not been released yet. While the Parliament has not yet voted on the proposal, it is expected that the matter will be scheduled for a first reading in the Parliament during the first half of 2015.

### III. Topics For Discussion

- A. Are trade secrets deserving of greater protection?
- B. Are there significant issues with the existing laws?
- C. Is uniformity desirable and obtainable?
- D. What basic components should be part of any uniform legislation?
- E. What remedies should be universal? Seizure orders?