SEYFARTH SHAW

Management Alert

Latest Updates on Federal Trade Secrets Legislation

By Robert B. Milligan and Amy Abeloff

With increased activity regarding proposed federal trade secrets legislation expected next month and for the remainder of the fall Congressional session, Seyfarth Shaw's dedicated Trade Secrets group has created a resource which summarizes the proposed legislation, outlines the arguments in favor of and against the legislation, and provides additional resources for our readers' convenience. This page will be continuously updated as we monitor and keep you apprised of the most recent developments, debate, and news regarding the legislation.

Below we provide an overview of trade secret law and the proposed federal legislation, the arguments on both sides of the debate, and our most current resource links.

How Are Trade Secrets Currently Protected?

Trade secrets are legally protectable information and can include a formula, pattern, compilation, program, device, method, technique or process. To meet the most common definition of a trade secret, a trade secret has three parts: (1) information; (2) reasonable measures taken to protect the information; and (3) which derives independent economic value from not being generally known. Examples of trade secrets include: plans, designs, negative information, computer software, customer lists, non-public financial information, cost and pricing information, manufacturing information, confidential information about business opportunities, and certain personnel information.

Trade secrets are generally protected by state law under a particular state's adoption of 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 and social media 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.

What is the Proposed Legislation?

On July 29, 2015, with bipartisan support, Congressional leaders in both the House and Senate, including Senators Orrin Hatch (R-UT), Christopher Coons (D-DE) and Representative Doug Collins (R-GA), introduced bills to create a federal private right of action for the misappropriation of trade secrets. The identical bills are HR 3326 and S. 1890 and they were referred to their respective judiciary committee. The proposed legislation, titled the "Defend Trade Secrets Act of 2015" ("DTSA"), follows an unsuccessful attempt just last year to pass the "Defend Trade Secrets Act of 2014."

The proposed legislation would authorize a private civil action in federal court for the misappropriation of a trade secret that is related to a product or service used in, or intended for use in, interstate or foreign commerce. The proposed legislation features amendments from the 2014 bill and seeks to do the following: 1) create a uniform standard for trade secret misappropriation by expanding the Economic Espionage Act; 2) provide parties pathways to injunctive relief and monetary damages to preserve evidence, prevent disclosure, and account for economic harm to companies; and 3) create remedies for trade secret misappropriation similar to those in place for other forms of intellectual property.

The DTSA has some similarities with the Uniform Trade Secrets Act. The DTSA defines "misappropriation" consistently with the DTSA, and provides for similar remedies, including injunctive relief, compensatory damages, and exemplary damages and the recovery of attorneys' fees in the event of willful or malicious misappropriation.

The DTSA, however, differs from the UTSA in several important aspects. Most notably, it opens the federal courts to plaintiffs for trade secrets cases. The DTSA also allows for an ex parte seizure order. A plaintiff fearful of the propagation or dissemination of its trade secrets would be able to take proactive steps to have the government seize its trade secrets prior to giving any notice of the lawsuit to the defendant. The proposed seizure protection goes well beyond what a court is typically willing to order under existing state law. Next, the DTSA's statute of limitations period is five years compared to just three under the UTSA. Additionally, the DTSA allows for the recovery of treble exemplary damages versus double under the UTSA. Finally, the DTSA contains no language preempting other causes of action that arise under the same common nucleus of facts, unlike the UTSA.

Do We Need Federal Trade Secrets Legislation?

Many business, professional, political, and academic leaders have called for the creation of a federal civil cause of action for trade secret misappropriation. There has been some vocal opposition to the legislation. Legislation to create a civil cause of action for trade secret misappropriation in federal court has failed in at least three previous attempts.

Recent scholarly articles in the Gonzaga Law Review and Fordham Law Review have suggested 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. David S. Almeling, Darin W. Snyder, Michael Sapoznikow, Whitney E. McCollum & Jill Weader, A Statistical Analysis of Trade Secret Litigation in State Courts, 46 gonz. l. rev. 57 (2011); David S. Almeling, Four Reasons to Enact a Federal Trade Secrets Act, 19 fordham intell. prop. media & ent. l.j. 768 (2009).

Additionally, published reports indicate that there is a growing rise in trade secret theft from foreign hackers, nation states, 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 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.

Another case involved the sentencing of a former DuPont employee who allegedly conspired with a South Korean company, Kolon Industries, to misappropriate trade secrets involving Kevlar, a well-known synthetic fiber product produced and sold by DuPont. Kolon Industries allegedly put a plan in place to recruit former DuPont employees so Kolon could create a product to compete with Kevlar without putting the time, effort, and expenditures into developing its own product. The former employee, even though he signed a non-disclosure agreement while at DuPont, allegedly retained DuPont documents upon his departure and turned them over to Kolon when they recruited him. Upon finding out about this scheme, the FBI investigated Kolon, and five of its executives were indicted for committing trade secret theft. Kolon plead guilty and was sentenced to pay $85 million in penalties and $275 million in restitution.

There is also significant harm caused by economic espionage committed by insiders. An employee of a large U.S. futures exchange company plead 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 FBI has recently launched a nationwide awareness campaign and released a short film based upon an actual case, The Company Man: Protecting America's Secrets, aimed at educating anyone with a trade secret about the threat and how they can help mitigate it. The film illustrates how one U.S. company was targeted by foreign actors and how that company worked with the FBI to address the problem.

From the perspective of those in favor of the legislation, 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, including what are reasonable secrecy measures. 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 statutes 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. Obtaining necessary service of process and discovery can be extremely difficult or impossible under the current system.

Proponents and Sponsors of the Bills

Announcement of the proposed legislation on July 29, 2015 was joined by a letter of support on behalf of the Association of Global Automakers, Inc., Biotechnology Industry Organization (BIO), The Boeing Company, Boston Scientific, BSA | The Software Alliance (BSA), Caterpillar Inc., Corning Incorporated, Eli Lilly and Company, General Electric, Honda, IBM, Illinois Tool Works Inc., Intel, International Fragrance Association, North America, Johnson & Johnson, Medtronic, Micron, National Alliance for Jobs and Innovation (NAJI), National Association of Manufacturers (NAM), NIKE, The Procter & Gamble Company, Siemens Corporation, Software & Information Industry Association (SIIA), U.S. Chamber of Commerce, United Technologies Corporation and 3M. The joint letter expressed the need for a private right of action to supplement the existing Economic Espionage Act of 1996 ("EEA"), which only provides for criminal sanctions in the event of trade secret misappropriation.

In 2014, two similar trade secret bills were introduced and received support from various constituents.

The Heritage Foundation 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 with the PRATSA bill. Also, a diverse set of companies and organizations have previously came 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, National Association of Manufacturers, and the National Chamber of Commerce.

Proponents of the bills have cited the advantages of a federal cause of action, and 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 complementary measure to combat trade secret misappropriation by private industry in light of strained government resources. A federal cause of 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, came out in favor of the 2014 house 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."

Opposition To The Bills

Last August, a group of 31 professors throughout the United States who teach and write about intellectual property law, trade secret law, invocation and/or information submitted an Opposition Letter to the 2014 bills. The professors cited 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. Following the letter, a Washington and Lee University School of Law professor, Christopher Seaman, critiqued the federalization of trade secrets law.

Shortly after the introduction of the bills in July, law professors David Levine and Sharon Sandeen wrote a new letter to Congress setting forth seven differences between the 2014 bills and the 2015 bill while still contesting the arguments of the

bill's supporters. The seven differences include: 1) the wrong is defined differently; 2) the ex parte civil seizure still remains but with apparently more stringent standards; 3) new encryption language has been added; 4) new concerns about employee mobility; 5) trade secrets are described as not intellectual property; 6) reporting of trade secret theft abroad is unclear as to whether it means "theft" or "misappropriation;" and 7) the "Sense of Congress" provision, which presumes trade secret theft is always "harmful." They believe that the recently introduced legislation does not ameliorate the problems it seeks to fix.

Current Status Of Proposed Legislation

Both bills have been introduced into their corresponding judiciary committee. HR 3326 and S. 1890 were introduced into committee on July 29, 2015.

For additional news and resources, please click here.

Robert B. Milligan is the Co-Chair of the Trade Secrets, Computer Fraud and Non-Competes Practice Group and the editor of the firm's Trading Secrets blog. Amy Abeloff is a law clerk in the firm's Los Angeles office. For more information, please contact your Seyfarth Shaw LLP attorney, Robert B. Milligan at rmilligan@seyfarth.com or Amy Abeloff at aabeloff@seyfarth.com.