Hearing on

"Trade Secrets: Promoting and Protecting American Innovation, Competitiveness and Market Access in Foreign Markets"

U.S. House of Representatives Committee on the Judiciary
Subcommittee on Courts, Intellectual Property and the Internet

June 24, 2014

Written Statement of Richard A. Hertling
Of Counsel
Covington & Burling LLP

Testimony of Richard A. Hertling
Of Counsel, Covington & Burling LLP
"Trade Secrets: Promoting and Protecting American Innovation, Competitiveness and Market Access in Foreign Markets"
June 24, 2014

Introduction and Summary

Good afternoon Chairman Coble, Ranking Member Nadler, and Members of the Subcommittee. Thank you for inviting me to testify today on trade secrets. It is a distinct honor and privilege to be here to discuss this very important topic.

As you know, my name is Richard Hertling, and I am of counsel to the Washington law firm of Covington & Burling LLP. Immediately prior to joining the firm, I was staff director of this committee, the capstone of my more-than-27-year career in federal service.

I am pleased to submit this testimony on behalf of Protect Trade Secrets Coalition, a cross-sector group of companies that is working to protect and defend trade secret property by supporting a harmonized, federal civil remedy for trade secret misappropriation.[1] The Coalition supports the Defend Trade Secrets Act, the bipartisan bill introduced by Senators Coons and Hatch. The Coalition appreciates this Committee's interest in trade secret protection and would support efforts to bolster the viability of and the protection accorded to the property interest that businesses have in their trade secrets by providing for civil jurisdiction in federal court for the misappropriation of a trade secret to complement the criminal jurisdiction and civil jurisdiction provided to the Attorney General in the Economic Espionage Act of 1996 ("EEA").

[1] Members of the Coalition include Abbott, Caterpillar, Corning Incorporated, Eli Lilly and Company, General Electric, Medtronic, Micron, Microsoft, Monsanto, NIKE, Pfizer, Philips, The Procter & Gamble Company, and United Technologies Corporation.

Trade secrets are commercially valuable information not generally known or readily ascertainable to the public by proper means that are subject to reasonable measures to protect the confidentiality of the information. The prototypical example of a trade secret at common law is the customer list, but trade secrets today may include high-tech manufacturing processes, industrial techniques, formulas, or complex data analytic algorithms. Trade secrets constitute roughly two-thirds of the value of companies' information portfolios and are an integral part of a company's competitive advantage, according to a recent Forrester Consulting report.[2]

American businesses are increasingly the targets of sophisticated efforts to steal proprietary information, harming our global competitiveness. Theft can come through cyber-attack, voluntary or involuntary disclosure by an employee, or misappropriation by a joint venture partner. Often the theft is state-sponsored. Government sources estimated more than a decade ago that the loss of intellectual property for American businesses from cyber espionage is $200 billion to $300 billion per year, and those figures are almost certainly higher today.[3]

The EEA, which made trade secret theft a federal crime, was Congress's first effort to protect American businesses' valuable trade secrets. As I will discuss, many of the problems that animated the passage of that law are of increasing concern today, including the ease with which trade secrets can be stolen using modern technology and the critical nature of trade secrets for our national economy and national security.

---

[2] Forrester Consulting, The Value of Corporate Secrets, at 2 (March 2010), *available at* http://www.nsi.org/pdf/reports/The%20Value%20of%20Corporate%20Secrets.pdf.

[3] Office of the National Counterintelligence Executive, *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage—2002*, NCIX 2003-10006 (Feb. 2003), *available at* http://www.fas.org/irp/ops/ci/docs/2002.pdf; National Bureau of Asian Research, Report of the Commission on the Theft of American Intellectual Property, at 11 (May 2013), *available at* http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.

I. The Economic Espionage Act of 1996

Trade secrets began to receive protection at common law during the middle of the 19th century. As there was scarcely a national market, much less an international market, the law governing and protecting trade secrets developed at the state level because with poor communications and transportation, trade secrets tended to be valuable only within a particular community.

The ad hoc pattern of 50 different state trade secret laws started to change in the 1980's, when states began to codify their laws by adopting the provisions of the Uniform Trade Secrets Act ("UTSA"), a model law developed and proposed to the states by the National Commission on Uniform State Laws. Today, 48 of the 50 states have enacted the UTSA, although often with a number of variances from the proposal, modestly undermining the goal of true uniformity.

It was against this background of state common law and then state statutory protection for trade secrets that the federal government ventured into the field to provide national protection for trade secrets. In 1995, the Department of Justice submitted to Congress a draft bill to make the misappropriation of commercial trade secrets a federal crime. The bill was born of a realization that the trade secrets of American businesses, which had become more and more important to the companies' prosperity, were increasingly under threat.[4] The threats came from disgruntled employees hoping to harm their former employers or turn profits for themselves by selling trade secrets; from outsiders targeting a company for theft; and, increasingly, from foreign governments using their espionage capabilities against American companies.[5]

---

[4] *See* H.R. Rep. No. 104-788, Economic Espionage Act of 1996, at 4-5 (1996).

[5] *Id.* at 5.

The Report from this Committee that accompanied the Economic Espionage Act of 1996 found that "the nation's economic interests are a part of its national security interests" and, thus, "threats to the nation's economic interests are threats to the nation's vital security interests."[6] The Director of the Federal Bureau of Investigation, Louis Freeh, testified before this Committee in 1996 that the FBI was investigating reports and allegations of economic espionage against U.S. companies by individuals or organizations from 23 different countries.[7] Despite the increasing attempts at trade secret theft and the challenges such theft posed to our economy, Director Freeh testified that the FBI faced difficulties in prosecuting trade secret theft cases because federal law did not specifically cover the misappropriation of trade secrets.[8] In some cases, the FBI had conducted investigations only to have federal prosecutors decline to prosecute because of a lack of statutory criminal authority to do so.

The EEA was designed to address that gap in federal criminal law. While federal law had long protected patents, copyrights and trademarks, trade secrets had been left unprotected, even though, as the House Report found, they form "an integral part of America's economic well-being."[9] The House found that state laws "do not fill the gaps left by federal law," because of the limitations of state laws.[10] "These problems underscore the importance of developing a systematic approach to the problem of economic espionage."[11]

---

[6] *Id.* at 4.
[7] *Id.*
[8] *Id.* at 6.
[9] *Id.* at 4.
[10] *Id.* at 6-7.
[11] *Id.* at 7.

The Senate Committee on the Judiciary also held hearings on what became the EEA and collected data. According to the Senate Judiciary Committee Report, "proprietary economic information is vital to the prosperity of the American economy, [ ] is increasingly the target of thieves, and [ ] our current laws are inadequate to punish people who steal the information."[12] The Senate Judiciary Committee found that as a result of trade secret theft, "American companies have been severely damaged," losing millions of dollars, jobs, and market share.[13]

Ultimately, the EEA passed by a vote of 399-3 in the House and by unanimous consent in the Senate and is now codified at 18 U.S.C. § 1831 *et seq.* The EEA makes it a criminal offense to misappropriate a trade secret for the benefit of any "foreign government, foreign instrumentality, or foreign agent."[14] The act also criminalizes the misappropriation of a trade secret "that is related to or included in a product that is produced for or placed in interstate or foreign commerce."[15] And the act authorizes the Attorney General to initiate a civil action to obtain appropriate injunctive relief for a violation of the law.[16]

---

[12] S. Rep. No. 104-359, The Industrial Espionage Act of 1996, at 5-6 (1996).

[13] *Id.* at 9 (relying on report of the National Counterintelligence Center).

[14] 18 U.S.C. § 1831(a).

[15] *Id.* § 1831(b).

[16] *Id.* § 1836. Towards the conclusion of Senate consideration of the EEA, a number of businesses requested that the bill include a federal civil remedy for the misappropriation of a trade secret to complement the bill's criminal provisions and the civil injunctive remedy it provided to the Attorney General. That request was made when the process was quite advanced and a general consensus surrounding the Senate bill had been reached. The provision was not included because it was raised too late in the process, but the thought was that the Congress could turn to that issue the following year. It was seen as a potentially valuable addition, but one that needed to be vetted on its own. For a variety of reasons, primarily that congressional attention on intellectual property issues was next absorbed by the subject that led to enactment of the Digital Millennium Copyright Act and subsequently by patent reform, the addition of a private federal civil remedy was not taken up following enactment of the EEA and lay dormant for a number of years thereafter, only to be renewed recently by members of both chambers, including members of this committee.

II. Recent Legislation

At the end of last Congress, this Committee was responsible for enacting two important laws to strengthen enforcement of trade secret laws. The Foreign and Economic Espionage Penalty Enhancement Act of 2012, P.L. 112-269, introduced by then-Chairman Smith increased penalties specifically for trade secret theft under the EEA for crimes that the perpetrator knows or intends to benefit a foreign government, instrumentality or agent. Fines for individuals were increased from a maximum of $500,000 to $5 million, and fines for organizations were increased to $10 million or three times the value of the stolen trade secret, including expenses for research and design. A House Report on the bill explained that "[b]y strengthening penalties and enhancing criminal deterrence, the bill protects U.S. jobs and technologies while promoting investments and innovation."[17] The House Report recognized the "significant and growing threat presented by criminals who engage in espionage on behalf of foreign adversaries and competitors."[18]

Congress also sent to the President the Theft of Trade Secrets Clarification Act of 2012, P.L. 112-236, which clarified the scope of the EEA to overturn the Second Circuit's decision in *United States v. Aleynikov*, 676 F.3d 71 (2d Cir. 2012), but made sure that the EEA continued to apply only to trade secrets related to products or services used in interstate commerce.

These recent legislative successes are important and promising steps to strengthening U.S. trade secrets law, and they have created an environment in which trade secrets are recognized as critical intellectual property entitled to the protection of federal laws in addition to the state laws that have traditionally protected them. They still have not put trade secrets — so

[17] H.R. Rep. No. 112-610, Foreign and Economic Espionage Penalty Enhancement Act of 2012, at 2 (2012).

[18] *Id.* at 1.

valuable to America's most innovative companies — on par with other forms of intellectual property, including patents, trademarks, and copyrights, all of which enjoy protection under a federal civil remedy. Owners of those other forms of intellectual property can protect what is rightfully theirs by taking action in federal court under the patent, copyright, and trademark laws.

Recognizing the value of American trade secrets, Congress has also approved free trade agreements that include specific protections for trade secrets. The U.S.-Colombia Trade Promotion Agreement, for instance, which took effect on May 15, 2012, contains explicit trade secret protections for pharmaceutical and agricultural products, as well as other intellectual property rights protections.[19]

III. Congress Should Enact a Federal Civil Remedy for the Misappropriation of Trade Secrets

The EEA, as amended last Congress, provides an important tool in fighting the theft of trade secrets and demonstrates a commitment by Congress to aid in protecting this vital form of U.S. intellectual property. Since enactment of the EEA, the problem of trade-secret theft has grown dramatically. Foreign competitors of U.S. business are trying to steal their way to success on the back of intellectual property developed here in the U.S. Although the EEA has been used successfully in many instances, the FBI has several priorities and limited resources and, as a result, cannot always respond to reports of the theft of a trade secret, even by foreign individuals and firms. Just as we as a society rely on both criminal law and the complementary tools of civil legal process to allow parties to protect their property interests, we should do so in this arena as well.

[19] *See* M. Angeles Villarreal, Cong. Research Serv., RL34470, The U.S. Colombia Free Trade Agreement: Background and Issues, at 5 (2014).

The methods thieves use in their attempts to steal American trade secrets are growing more sophisticated by the day, and our laws must keep pace. American businesses that compete globally will lose their competitive edge — and put at risk thousands of well-paying U.S. jobs — if they cannot quickly pursue and stop thieves who steal their hard-earned secrets to sell to the highest foreign bidder. Federal law must provide our country's innovators and job creators with the tools they need to keep their trade secrets from falling into the wrong hands. The failure to do so risks the global competitiveness of the U.S. economy, which more than ever depends on our innovative intellectual property to provide our competitive advantage over foreign businesses.

Civil trade secret laws originated at the state level, in an era when trade secret theft was largely a local matter. State trade secret laws work well when, for instance, an employee of a local business steals a customer list and takes it to the business down the street. For companies that operate across state and national borders and have their trade secrets threatened by competitors around the globe, the array of state laws is inefficient and inadequate for several reasons.

First, companies need compliance plans to protect their trade secrets. Under the array of state laws, a company that operates in more than one state bears additional and unnecessary costs to protect this form of intellectual property. Second, trade secret theft today is increasingly likely to involve the movement of the secret across state lines. Such multi-jurisdictional movement makes discovery and service of process difficult. Federal courts permit subpoenas to be issued nationwide, but state courts are often not as efficient at obtaining discovery in other states. And third, trade secret cases require swift action by courts across state lines to preserve evidence and protect the trade secret from being divulged. This is particularly true when the

theft is by an individual looking to flee the country, as is increasingly the case. State courts lack the ability of the federal system to serve defendants and prevent the disclosure of the trade secret or destruction of evidence.

Once a trade secret has been divulged, or is made known to a competitor, trade secret protection may be lost forever and the harm from disclosure is often irreparable. Given the mobility we enjoy today, the ease with which people and information travel across state and national borders, relying on disparate state laws and procedures is no longer adequate for the protection of trade secrets in the 21st century. The world of business has changed dramatically in a decade, not to mention since trade secret laws were first developed in the 19th century. U.S. businesses need remedies that enable them to respond immediately and effectively across state lines to protect their trade secrets.

The Senate is considering the Defend Trade Secrets Act, S. 2267, which will create a uniform federal civil remedy for trade secret misappropriation and provide a mechanism to obtain expedited relief when there is a threat that stolen U.S. trade secrets are about to be disclosed or the evidence destroyed. A consistent, harmonized legal framework will provide a more efficient and effective legal structure to protect the valuable intellectual property of American businesses and help protect and promote U.S. global competitiveness and preserve high-quality U.S. jobs. It will also put trade secret protection in-line with the remedies available for owners of other forms of intellectual property. Further, by creating a uniform standard, the legislation will encourage companies to create one set of best practices to protect their trade secrets in every state.

IV. Conclusion

In the information age, knowledge and innovation are our greatest strengths as a country. But for that same reason, they are also the target of sophisticated thieves hoping for a quick

payday on the backs of American businesses. A federal civil remedy for trade-secret theft would provide an important addition to existing protections for trade secrets at the federal and state levels and could potentially bolster our economy at no additional cost.