STATEMENT OF PROFESSOR SHARON K. SANDEEN[1]

BEFORE THE

UNITED STATES SENATE

COMMITTEE ON THE JUDICIARY

ON

"Protecting Trade Secrets: the Impact of Trade Secret Theft on American Competitiveness and Potential Solutions to Remedy This Harm."

December 2, 2015

I. INTRODUCTION

Thank you Chairman Grassley, Ranking Member Leahy and the other members of the Senate Judiciary Committee.

I am honored to be here today. I am a professor of law at Hamline University School of Law (subject to the acquiescence by the ABA, soon to be Mitchell Hamline School of Law). I am also the author of numerous books and articles on the topic of United States and international trade secret law, including the first trade secret law textbook for law school use. I am also a former civil litigator, having worked in that capacity for 15 years before becoming a law professor. In fact, it was my experiences as a litigator that drew me to focus my scholarship on trade secret law and information policy.

For the record, I am against the misappropriation of legitimate trade secrets and fully support the existing set of state laws and the existing federal criminal statute that are designed to protect such secrets. I also agree that the problem of cyberespionage is serious and is an appropriate issue for Congress to address. However, the Defend Trade Secrets Act does not directly address the problem of cyberespionage and I believe its costs are greater than its marginal and debatable benefits.

[1] Prepared by Sharon K. Sandeen, Professor of Law, Hamline University School of Law, St. Paul, Minnesota and David S. Levine, Associate Professor of Law, Elon University School of Law, Greensboro, North Carolina. David S. Levine is an Affiliate Scholar at Stanford Law School's Center for Internet and Society and a Visiting Research Collaborator at Princeton's Center for Information Technology Policy. He has written several articles on trade secrecy and information access, and was a civil litigator in intellectual property and other related fields for seven years before entering academia.

You [have heard/ will hear] from multiple presenters about the problems of trade secret misappropriation and cyberespionage from the perspective of large, multi-national corporations that have been victimized by the wrongful acquisition of their trade secrets.

I will speak from a perspective that has not been adequately represented in discussions about the D.T.S.A., that of numerous start-up companies, entrepreneurs, mobile employees, and small and medium-sized businesses that are sued for trade secret misappropriation and forced to defend themselves, often when there are no legitimate trade secrets or little or no evidence of misappropriation.

I am happy that over 40 law professors from across the country have joined me and my co-authors in expressing their concerns in two letters written in opposition to the proposed legislation.[2]

II. The Vast Majority of Trade Secret Cases Are Brought Against Former Employees, Not Spies

Although much of the commentary that surrounds the D.T.S.A. concerns the problem of cyberespionage, the vast majority of trade secret claims in this country are not against alleged spies but involve former employees or other business associates.[3]

This is where the potential for abuse arises. Usually in these cases, the alleged misappropriation does not involve the wrongful acquisition of trade secrets, but rather an alleged breach of a duty of confidentiality.[4] In other words, in most trade secret cases the defendant was voluntarily given access to the alleged trade secret by his or her own employer or business associate, sometimes under circumstances giving rise to a duty of confidentiality, sometimes not.

The companies that support the D.T.S.A. are very sophisticated, have ample legal resources, and have detailed policies and procedures in place to identify and protect their trade secrets. However, not all trade secret plaintiffs fall into that camp.

Often, businesses do not even know that they might have trade secrets until a former employee leaves to go to work for a competitor or to start a competitive business. When the

[2] Professors' Letter in Opposition to the "Defend Trade Secrets Act of 2014" (S. 226) and the "Trade Secrets Protection Act of 2014" (H.R. 5233) (Aug. 26, 2014), *available at* http://cyberlaw.stanford.edu/files/blogs/FINAL%20Professors'%20Letter%20Opposing%20Trade%20Secret%20Legislation.pdf [hereinafter "2014 Professors' Letter"] and Professors' Letter in Opposition to the "Defend Trade Secrets Act of 2015" (S. 1890, H.R. 3326) (Nov. 7, 2015), *available at* https://cyberlaw.stanford.edu/blog/2015/11/new-professors-letter-opposing-defend-trade-secrets-act-2015.

[3] David Almeling, et. al., *A Statistical Analysis of Trade Secret Litigation in State Courts*, 46 GONZAGA. L.R. 57, 59-60 (2010); David Almeling, et. al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 GONZAGA. L.R. 291, 303 (2009).

[4] *See* UNIF. TRADE SECRETS ACT § 1(2) (UNIF. LAW COMM'N 1985), definition of "misappropriation."

former employer hires an attorney, the former employee finds out – after the fact – that she may be involved in trade secret misappropriation.

Where legitimate trade secrets exist and there is evidence of misappropriation, I have no problem with litigation brought against former employees. However, I am against the mis-assertion of trade secret rights, including for the purpose of disrupting a competitor or to punish a former employee who has a great new idea and some entrepreneurial initiative. This is what my co-author, David Levine, and I refer to as the "Trade Secret Troll" problem, which is akin to, but (as we explain in our article) not identical to, the patent troll problem.[5]

Misunderstandings about the true scope of trade secret rights and the limited types of behaviors that constitute misappropriation help explain why many trade secret cases are unsuccessful. The lack of success is not because the existing trade secret law in the United States is inadequate, but because the putative trade secret owner either did not have legitimate trade secrets or cannot prove that they were misappropriated.

III. There Are Important Reasons Why Trade Secrets Rights Are Limited

When considering whether the D.T.S.A. actually addresses cyberespionage, it is important to understand that trade secret law does not protect all business information. It does not even protect all secret business information. It only protects a subset of secret business information which can meet trade secrecy's stringent legal requirements.[6]

Trade secret doctrine has long recognized that information that is known by both the general public, or within a particular industry, cannot be a trade secret. Trade secret law also does not protect the general skill and knowledge that employees learn on the job, often including highly specialized knowledge and skills.

Unfortunately, many trade secret plaintiffs do not understand these limits. They also do not understand that it is not "wrong" for companies to engage in legitimate competitive intelligence, reverse engineering, and independent development. These are some of the ways that businesses stay competitive and are able to offer consumers better products and lower prices.

[5] *See* David S. Levine and Sharon K. Sandeen, *Here Come the Trade Secret Trolls*, 71 Wash. & Lee L. Rev. Online 230 (2014), fn. 1 and related text.

[6] *See* UNIF. TRADE SECRETS ACT § 1(4) (UNIF. LAW COMM'N 1985), defining a "trade secret" as information that is: (1) secret; (2) has independent economic value; and (3) is the subject of reasonable efforts to maintain its secrecy.

There are important reasons for the limitations on the scope of trade secret protection. First, there is the strong public policy, repeated in numerous Supreme Court cases,[7] that the law cannot (and should not) protect information that is in the public domain.

Additionally, there is a longstanding policy that inventors should seek patent protection rather than keeping their inventions as trade secrets. As the U.S. Supreme Court stated, trade secret protection must be limited because otherwise it interferes with the patent policy of disclosure of information upon which others can ultimately build.[8]

The D.T.S.A., when coupled with recent changes to patent law as a result of the America Invents Act, threatens to disrupt this longstanding policy.[9] Enabling companies to threaten federal trade secret litigation - particularly with respect to formulas and processes that can be used while still being kept hidden - will undermine the disclosure purposes of both U.S. patent law and state trade secret laws. The net result will be a reduction in access to and diffusion of information and knowledge in this country,[10] possibly less innovation, and certainly more litigation.

In other words, the public interest will be harmed.

IV. Trade Secret Litigation Is Expensive and Will Be Even More Expensive Under the Defend Trade Secrets Act

There are a number of reasons why the D.T.S.A. will increase litigation costs, costs that small businesses that are wrongfully accused of trade secret misappropriation can ill-afford.[11]

First, as there is no federal civil trade secret jurisprudence, numerous issues that have long been resolved at the state level are sure to be highly litigated at the federal level. As the

---

[7] *See e.g,* Sears, Roebuck & Co. v. Stiffel Co., 376 U.S. 225 (1964); Compco Corp. v. Day-Brite Lighting, Inc., 376 U.S. 234 (1964); Bonito Boats Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141 (1989).

[8] Kewanee Oil Co. v. Bicron Corp, 416 U.S. 470 (1974).

[9] The case of Metalizing Eng'g Co. v. Kenyon Bearing & Auto Parts Co., 153 F. 2d. 516 (2d Cir 1946), established the principle (now known as the Metalizing Doctrine) that an inventor cannot make commercial use of an invention, even in secret, and later seek to patent the invention after the expiration of the applicable grace period. While there is little legislative history surrounding the AIA to support the assertion that Congress intended to statutorily overrule the Metalizing Doctrine, some proponents of the AIA have urged such an interpretation. Those that do also have an interest in stronger trade secret protection that, because of the issues of federal preemption discussed in *Kewanee*, can only be accomplished through the adoption of federal trade secret legislation.

[10] For general discussion about the impact of trade secret law on access to information, *see* David S. Levine, *Secrecy and Unaccountability: Trade Secrets in our Publfic Infrastructure*, 59 FLA. L. REV. 135 (2007) (explaining how the aims of secrecy sometimes conflict with "the methods and purpose of transparent and accountable democratic governance").

[11] Sharon K. Sandeen, *The DTSA: The Litigator's Full-Employment Act*, 72 Wash. &. Lee L. Rev. Online (forthcoming 2015).

federal courts develop their jurisprudence, they will have multiple sources of existing state law to borrow from,[12] but with no direction from Congress on which to choose.

I favor the Uniform Trade Secret Act which has been adopted in 47 of 50 states, but federal judges may go a different direction, thereby leading to less uniformity in trade secret doctrine, not more. I am particularly concerned that many of the well-established principles of trade secret law that are discussed in the comments to the UTSA are not included in the proposed legislation.

I am also concerned about how the federal courts might address the so-called inevitable disclosure doctrine and other employment-related issues that often arise in trade secret cases, such as the enforceability of noncompete agreements. As a native of northern California, I have witnessed first-hand how California benefited from the mobility and entrepreneurial spirit of its workforce. Many argue that Silicon Valley would not be so successful were it not for the long-standing policy of California that holds noncompete agreements unenforceable except in very limited circumstances.[13]

Having employees learn on the job and then believe that they can build a better business is the American Way and is what keeps many employees engaged and striving for a better life. Unfortunately, today, start-up companies can easily find themselves as defendants in all manner of alleged IP infractions. For example:

- They pick a name for their business, only to receive a cease-and-desist letter alleging trademark infringement;
- They purchase a printer for use in their business and they get sued for patent infringement;
- They download software to fix the printer, and they are accused of copyright infringement;
- They use information they learned on the job, arguably general skill and knowledge, and they get sued for trade secret misappropriation.

These are the real-world consequences for U.S. businesses of ever-expanding IP rights and remedies. Although, in theory, weak or illegitimate claims will be exposed during the course of litigation, many small businesses, start-ups, and mobile employees cannot afford to litigate. Instead, they are forced to simply capitulate.

[12] This includes: (1) the Restatement (First) of Torts provisions governing trade secrecy; (2) the Uniform Trade Secrets Act; (3) the Restatement (Third) of Unfair Competition provisions governing trade secrecy; and (4) the trade secret jurisprudence of fifty states.

[13] *See, i.e.,* AnnaLee Saxenian, *Regional Advantage: Culture and Competition in Silicon Valley and Route 128* (Cambridge, MA: Harvard University Press 1994).

The D.T.S.A.'s jurisdictional clause will be highly litigated for the simple reason that trade secrets are not used openly or in ways that their connection to interstate commerce can be seen and easily tested. Since the existence of trade secrets and their use in interstate commerce is a Constitutional requirement, one can expect numerous motions and debates on the issue of federal court jurisdiction, including a lot of early and costly discovery.

The proposed civil seizure provision will also be highly litigated, particularly since it is a tool that plaintiffs can use to shut down a competitor's business. Although this concern was addressed somewhat compared to the legislation introduced last session, what remains is a highly complex and troublesome remedy that is fraught with potential abuse.[14] It is particularly troublesome when one considers that many plaintiffs in trade secret cases do not have strong claims but the ex parte nature of the remedy means that there will be no one to point out such weaknesses.

V. There Are Better and More Direct Ways to Address the Cyberespionage Problem

I believe that the Defend Trade Secrets Act is well-intentioned. I share the sponsors' concerns about cyberespionage and the misappropriation of legitimate trade secrets by foreign operatives. However, I think there are better ways to address those problems.

For one, if the intent of the law is to stop the wrongful acts of cyberespionage and other forms of spying, why would we want to make the existence of a legitimate trade secret a predicate fact? Isn't the real concern the bad acts that lead to the improper acquisition of confidential business information, regardless of whether that information qualifies as a trade secret?

We already have a federal law on the books with both criminal penalties and a civil cause of action that addresses the wrongful acquisition of information stored in a computer, known as the Computer Fraud and Abuse Act.[15] Why not amend that law to more directly address the bad acts of cyberespionage while at the same time solving the problem that the current law poses with respect to everyday Internet usage? This would differentiate the egregious cases of intentional espionage from cases that involve ill-informed former employees and Internet users.[16]

There are also better and more direct ways to address some of the procedural problems that the proponents of the D.T.S.A. use to justify the legislation. For instance, Congress could exercise its powers under the Full Faith and Credit Clause of the Constitution and direct state

[14] Eric Goldman, *Ex Parte Seizures and the Defend Trade Secrets Act*, 72 Wash. &. Lee L. Rev. Online (forthcoming 2015).

[15] 18 U.S.C. §1030.

[16] For more discussion of proposed alternatives, *see Here Come the Trade Secret Trolls*, *supra note* 5. *See also*, Christopher B. Seaman, *The Case Against Federalizing Trade Secrecy*, 101 Va. L. Rev. 317, 385-90 (2015).

courts to more readily recognize and enforce orders and judgments entered by other courts in trade secret cases.[17] There may also be ways for Congress to make interstate discovery easier, helping all state court litigants and not just trade secret litigants.

In conclusion, the D.T.S.A.'s proponents have not made the case for the federal expansion of trade secret law, particularly in light of the fact that we already have a robust set of state laws and many trade secret cases are already filed in federal courts based upon diversity jurisdiction.

If anything is clear, it is that more laws are not necessarily better, particularly when a proposed law is largely duplicative of existing state laws and when the proposed law will increase the costs of litigation and has the potential for significant abuse.

Because disrupting established trade secret principles and the legitimate business operations of start-up companies, small and medium sized enterprises, and mobile employees is the most likely outcome of the D.T.S.A., it should be rejected.

Thank you for your time and attention. I would be happy to answer any questions.

oOo

[17] For an example of this strategy with respect to protection orders issued in domestic violence cases, see 18 U.S.C. §2265.