August 3, 2015

VIA EMAIL TO THE SPONSORS OF THE DEFEND TRADE SECRETS ACT

An open letter to the sponsors of the revised Defend Trade Secrets Act:

We write to express our continued concerns about the Defend Trade Secrets Act ("DTSA") and our willingness to assist you in determining how best to improve enforcement of legitimate trade secret rights. In August 2014, 31 academics signed a letter raising many concerns with similar legislation then pending in the House and Senate. We attach a copy of that letter, which can be found at http://cyberlaw.stanford.edu/files/blogs/FINAL%20Professors'%20Letter%20Opposing%20Trade%20Secret%20Legislation.pdf (the "August 2014 letter").

In the July 29, 2015 press release announcing the new DTSA, the sponsors again identify the harm that they seek to address, namely, that "trade secrets can be stolen with a few keystrokes, and increasingly, they are stolen at the direction of a foreign government or for the benefit of a foreign competitor." To justify the DTSA, the release argues that (a) current federal criminal law is "insufficient," (b) the Department of Justice "lacks the resources" to prosecute (presumably) Economic Espionage Act ("EEA") cases, (c) state law has not stopped "interstate" theft, and (d) Federal courts would be more effective in case administration and discovery. Thus, the release says that the DTSA would "harmonize" United States law, "provide for injunctions and damages," and make trade secret law "consistent" with existing federal intellectual property law, which we understand to mean simply that there would now be a federal private trade secret cause of action. Presumably, the sponsors believe that these outcomes are needed, and would address cyber-misappropriations of trade secrets.

Indeed, these are the general arguments that were proffered in support of last year's legislation. In response, the undersigned addressed these assertions in detail in a January 2015 article published in the *Washington and Lee Law Review Online*, titled "Here Come the Trade Secret Trolls," which can be found at http://lawreview.journals.wlu.io/here-come-the-trade-secret-trolls/ (the "January 2105 article"). In the January 2015 article, we concluded that the DTSA does "not address, much less solve," the *exact* cyberespionage harm quoted above. Instead, we explained, the DTSA has many downsides, and is "most likely to spawn a new intellectual property predator: the heretofore unknown 'trade secret troll,' an alleged trade secret owning entity that uses broad trade secret law to exact rents via dubious threats of litigation directed at unsuspecting defendants."

Unfortunately, the new DTSA appears to simply combine many of the provisions of the two pieces of legislation that were introduced in 2014 (S. 2267 and H.R. 5233). As a result, it addresses few of the concerns raised in the January 2015 article and the August 2014 letter. Moreover, the sponsors have failed to explain how the DTSA improves existing trade secret law, nor how it will specifically address the harms that it purports to mitigate. Thus, the August 2014 letter and January 2015 article remain highly relevant to an analysis of the DTSA's benefits and drawbacks.

As with previous bills, the new DTSA would amend the EEA to include a private cause of action for trade secret misappropriation that is principally modeled on the Uniform Trade Secret Act ("UTSA"). Thus, the new DTSA is very similar to last year's legislation. However, it has seven important (and potentially problematic) differences. The following is our quick understanding of how the new DTSA compares to the Senate version of the DTSA that was introduced last year. If we misunderstand these changes, we welcome your reply.

1. **The wrong is defined differently.** Last year's DTSA created a private cause of action for the wrongs already defined in the EEA, which generally required heightened proof over what the UTSA required because of the *mens rea* requirement that is a part of the current EEA, a criminal statute. This year's version takes from last year's House version to provide a private cause of action by "a person aggrieved by a misappropriation of a trade secret that is related to a product or service used in or intended for use in, interstate or foreign commerce."

This clause appears to serve two basic purposes. First, it defines who has standing to sue. Second, it is designed to meet the Constitution's Commerce Clause requirement of regulating interstate commerce.

With respect to the first purpose, it appears that the intent of Congress is to grant standing to persons who are harmed by acts of trade secret misappropriation, but we are concerned that the required harm is not clearly defined. Typically, United States law does not provide a civil claim for relief unless there are measurable and demonstrable damages or, in the case of injunctive relief, a real threat of future harm. As with last year's bill, the wrongful act is defined as "misappropriation" and "misappropriation" is defined in language that mirrors the UTSA. If the "person aggrieved" means the party that suffers actual (or threatened) harm caused by an act of misappropriation (as defined), then the need of trade secret owners to prove actual harm is preserved. However, if it means something less than actual harm, the new DTSA would mark a significant and unwarranted departure from long-standing principles of U.S. law.[1]

With respect to the second purpose, the fact that federal trade secret legislation must be based upon the Commerce Clause power means that state law claims will continue to exist. Thus, far from creating more uniformity, the proposed legislation will result in *less* uniformity as the federal judiciary will have to develop its own trade secret jurisprudence. More immediately, the proposed jurisdictional language is unclear, untested, and potentially overbroad. Therefore, it is likely to lead to a raft of costly motions to dismiss as defendants claim that their trade secrets do not "relate to a product or service used in or intended for use in interstate commerce."

[1] As discussed below, the "Sense of Congress" language that was added to this year's legislation only serves to heighten our concern that the new DTSA creates a cause of action akin to an emotional distress claim, instead of being grounded in a need to prove actual harm to the subject trade secret owner.

Of particular concern is the fact that the language does not focus on the putative trade secrets themselves and does not even try to identify the extent to which the required interstate products or services must be imbued with misappropriated trade secrets. The resulting questions that will have to be answered by courts will benefit only the lawyers collecting fees from their clients. For example, if trade secrets make up only one-percent of the product (say a cellphone), is that enough?

2. The ill-advised *ex parte* civil seizure remedy remains, but with more explicit and difficult requirements. The new DTSA's *ex parte* civil seizure remedy is arguably the most controversial provision, principally because, as we've previously emphasized, it is fraught with potential anti-competitive abuse. In an apparent effort to address these concerns, the new DTSA includes the more particular and lengthy provisions found in last year's House bill.

Wisely omitted from last year's DTSA is the "preservation of evidence" purpose for a seizure order, thereby deleting a "special" benefit that other civil litigants in federal court do not enjoy and that arguably can be obtained through existing rules of civil procedure. Added to this year's DTSA is a provision titled "Seizure Hearing" that provides some details concerning the hearing that must be held within seven days after a seizure order is granted. Also, there is additional language related to the requirement that the Court hold the seized material in its possession. Like last year's DTSA, the new DTSA includes a provision allowing for an action for damages in the case of wrongful seizure.

Despite the foregoing changes, our concerns as discussed in our January 2015 article remain. Because *ex parte* seizure is an unprecedented remedy that can be used to effectively shut-down legitimate competition, the DTSA is a bill fraught with danger to putative defendants, regardless of the merits of the allegations against them. Because *ex parte* seizure is likely to be an extremely expensive process for both the courts and the parties, start-up companies that are sued by larger companies might very well capitulate rather than incur the expense of costly procedural maneuverings. Thus, while the provision might look good on paper as a means to quell foreign cyber-espionage, in practice it will likely to have more of an adverse impact on U.S.-based entrepreneurs than on the foreign agents and cyber-hackers whose activities it is purportedly designed to address.

3. A motion for "encryption" has been added. With respect to seized material, the new DTSA provides that a party may make a motion at any time to encrypt seized material. Nothing in the new DTSA details who will pay for either the encryption or a court's holding of seized materials. It seems potentially counter-intuitive that materials held by a court (and presumably not resident on a computer server) would need to be encrypted.

4. Employee mobility concerns. As currently written, the new DTSA does not include several of the limitations on the scope of trade secret protection that, among other purposes, are designed to protect employee mobility (and which are explicitly included in the proposed European Union Trade Secret Directive). Nor does it take an explicit stand on the doctrine of inevitable disclosure, a highly controversial common law doctrine that can prevent employee mobility based upon the mere suspicion that information allegedly owned by another might be used in an anti-competitive way.

However, limiting language was added to the new DTSA's remedies provisions (which generally mirror the UTSA provisions) to require that injunctions cannot "prevent a person from accepting an offer of employment under conditions that avoid actual or threatened misappropriation." Although this language appears on the surface to favor employee mobility, in reality it just restates the difficult issue that is before a court when an inevitable disclosure argument is made. Indeed, it might be read to endorse the cause of action even though it has been soundly rejected by a significant cohort of states.

To the extent that the new DTSA gives any ammunition to the inevitable disclosure doctrine, we are very concerned about its impact on employee mobility, both for employees and the employers that seek to hire talented people. In this regard, the United States has a rich history of former employees who learned on their former jobs, had a better idea, and started new companies that grew, prospered and created new jobs. This behavior should be encouraged by U.S. policy, not hampered by overly restrictive trade secret laws.

5. Trade secrets are not intellectual property. The new DTSA includes language from last year's House bill which states: "This Section and the amendments made by this section shall not be construed to be a law pertaining to intellectual property for the purposes of any other Act of Congress." The purpose of this language is unclear, but not labeling trade secrets as intellectual property is consistent with the Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPS Agreement"), Article 39. Also, this language appears to highlight that the Constitutional basis for the legislation is the Commerce Clause (Article 1, Section 8, Clause 3) powers, and not its powers under the Progress Clause (Article 1, Section 8, Clause 8). Further study is needed to determine the ramifications of this provision.

6. Report on theft of trade secrets occurring abroad. Like last year's House version, the new DTSA includes a requirement for a regular report about trade secret theft occurring abroad. Interestingly, this provision repeatedly uses the term "theft" and not "misappropriation," leaving it unclear whether theft is different from misappropriation or is a subpart thereof. Similar reports, like the United States Trade Representative's Special 301 Report on the state of intellectual property rights outside the United States, tend to become political footballs, and we are unconvinced that they will be a valuable use of time or resources.

A better use of taxpayer money would be for the Federal government to assist United States businesses in identifying and protecting legitimate trade secrets and improving their own cybersecurity practices. An unfortunate fact is that much of the concern about trade secret misappropriation can be traced to sloppy industry practices. For example, encouraging United States manufacturers to keep their important trade secrets and related manufacturing processes within the United States, when possible, can be an effective cybersecurity strategy against foreign misappropriation. There is much work to be done on improving cybersecurity capabilities, and the United States government could be a positive contributor to those efforts if it so chooses.

7. Congress thinks trade secret theft is bad. Entirely new to the DTSA is the final section that is labeled "Sense of Congress." In sum, it states that Congress believes that trade secret theft occurs, and that whenever is occurs it "harms" the companies that own trade secrets.

This is troubling language because of its embedded assumption of harm, an issue that pervades the DTSA, new and old. Under traditional tort principles and the UTSA (and, in fact, language in the legislation that is borrowed from the UTSA), harm is not presumed from the act of misappropriation itself but must be *proven* as a separate element of the cause of action. Additionally, it is factually incorrect to assert that there are trade secret harms if they are not improperly disclosed or used. Congress should be concerned about various "bad acts," including hacking and cyber-espionage, but suggesting that trade secret misappropriation in the form of wrongful acquisition always results in harm would be an unwise and dangerous expansion of trade secret doctrine. **Therefore, the aforementioned concern about the DTSA giving rise to trolling behavior is amplified by the DTSA's assumption that harm always occurs whenever a trade secret is misappropriated.**

In sum, **all of our August 2014 letter and January 2015 article concerns remain**. Combined with an *ex parte* seizure remedy, embedded assumption of harm, and ambiguous language about the inevitable disclosure doctrine, the new DTSA appears to not only remain legislation with significant downsides, but those downsides may actually be even more pronounced. Moreover, the DTSA still does not do much, if anything, to address the problem of cyber-espionage that cannot already be done under existing state and federal law.

As Congress takes on the purported problem of patent assertion entities (also known as "trolls;" an issue on which we take no position), it should be aware of the very real possibility that the DTSA could create an entirely new form of troll. This new "trade secret troll" could cause significant harm to weaker and smaller businesses, as well as start-ups and fledgling entrepreneurs. **Thus, we urge Congress to abandon the DTSA.**

We remain committed to aiding you in your laudable efforts to help United States' individuals and businesses protect their legitimate trade secrets, and raise the foregoing concerns in that spirit. Thus, we ask that you **reconsider your support for the DTSA**. Moreover, in the event that the DTSA goes forward, we ask that there be **public hearings** on (a) the benefits and drawbacks of the DTSA, and (b) the specific question of whether the DTSA addresses the threat of cyber-espionage. Finally, we ask that you consider other possible ways to address cyber-espionage, including **amending the Computer Fraud and Abuse Act**, as outlined in our January 2015 article.

With regard to this letter, you may address any reply or correspondence to the undersigned, Professor David S. Levine (dsl2@princeton.edu) and Professor Sharon K. Sandeen (ssandeen@hamline.edu). For other critiques of last year's bills and the concept of federal trade secret legislation in general, please see the bibliography that can be found at http://blog.ericgoldman.org/archives/2015/04/a-bibliography-about-federal-trade-secret-law-reform-guest-blog-post.htm.

Signed,[2]

David S. Levine
Elon University School of Law
Visiting Research Collaborator
Center for Information Technology Policy, Princeton University
Affiliate Scholar
Center for Internet and Society, Stanford Law School

Sharon K. Sandeen
Hamline University School of Law
Co-author, *Cases and Materials on Trade Secret Law* (West Academic Publishing 2012) and *Trade Secrecy and International Transactions* (Edward Elgar 2015)

Attachments

[2] All institutions are listed for identification purposes only and the signatories do not speak for or on behalf of their respective institutions.