The Defend Trade Secrets Act: Arrival of the Trade Secret Trolls?

Stephen Anderson

INTRODUCTION

In today's world it is increasingly apparent that advancements in technology have allowed information to be shared, and to be stolen, more than ever before. This encompasses simple tweets, as well as information guarded and seemingly protected by small businesses and large corporations alike. There have been expected downsides with these technological capabilities, namely state-backed cyber espionage and trade secret misappropriation. A new bill that is currently facing Congress, the Defend Trade Secrets Act, is aimed at creating a federal private cause of action under the Economic Espionage Act of 1996 (EEA). It is a bill that will, if passed, expand the EEA to provide federal jurisdiction for the theft of trade secrets. There is no question as to the degree of importance the protection of trade secrets is to United States businesses and society at large. The question is whether the well-intentioned DTSA will actually do more harm than good. There are a substantial number of legal professionals that have voiced their concern that not only will it fail to significantly hinder cyber-espionage, but it will open the door to a new breed of predators, trade secret trolls.

I. Background

The very definition of a trade secret has been a point of confusion when discussing the DTSA and is therefore necessary to first define. The Uniform Trade Secrets Act defines a trade secret as "(1) information (2) that derives economic value from not being generally known or readily ascertainable through appropriate means by other persons who might obtain economic value from its disclosure and use; and (3) is the subject of efforts that are reasonable under the

circumstances to maintain its secrecy. [1] It is important to note that trade secrets do not include any and all information businesses keep secret and that the use of a trade secret does not always constitute misappropriation. [2] The trade secret must be acquired through improper means or involve a breach of confidence to be protected. [3] This distinction is something that has gotten lost in the current discourse surrounding this topic. It is also a necessary framework from which to discuss the DTSA and its implications, due to the difficulty to discern between routine employee behavior and actual trade secret misappropriation.

Another necessary distinction to understand is the two legal theories underlying trade secret law, tort and property. In order for a trade secret misappropriation to have taken place there needs to be the tort, i.e. the improper acquisition or breach, and the property interest, i.e. the information being misappropriated is definitively a trade secret. [4] Too often when DTSA is discussed there is an assumption that all business information is protected under trade secret law, when in reality it is not. Those in opposition of the DTSA consistently remark on the bill's "hyper-focus" on property and ownership. [5] They feel there is a necessity for the bill to examine trade secrecy as a tort-based concept. [6] Together the two theories build trade secret law to allow intellectual competition, while also preventing wrongful acts, such as misappropriation. The inappropriate focus on one theory will lead to harmful repercussions and, in this particular case, will lead to the arrival of trade secret trolls. [7]

There is little doubt that the DTSA is well intentioned and it is important to clearly lay out the reasons the bill is currently before Congress. Trade secrets are the only form of IP rights that do not have the protection of a federal private right of action. [8] The primary concern, according to the July 29, 2015 press release, is 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." [9]

Supporters state that current federal law in the field of trade secrecy is insufficient and present state law has not sufficiently stopped the issue. [10] Furthermore, they say the Department of Justice does not have the adequate resources to prosecute EEA cases and federal courts are better equipped to handle trade secrecy cases. [11] Despite these persuasive arguments, detractors continue to say that the DTSA does not solve the exact harm it is sets out to rid. [12] Rather, it opens the courts to a "free-ranging, plaintiff-oriented" legal system that has the tangible probability of creating trade secret trolls. Step by step legal scholars have pointed out the potential pitfalls of the DTSA and continue to ask for its denial. [13]

The most contentious section of the bill surrounds the *ex parte* civil seizure remedy. [14] This remedy is unique to the DTSA, in that it goes far beyond what a court is willing to do under existing state law. [15] Specifically, this remedy allows a plaintiff to obtain a court order at the outset of the case and proceed against a defendant who is allegedly in possession of the privileged goods and seize those goods, without any notice to the defendant. In order to meet the requirements to enforce the *ex parte* remedy, the DTSA states the applicant must show that the information is a trade secret and the person against whom seizure would be ordered did the following:

> "[M]isappropriated the trade secret by improper means; conspired to use improper means to misappropriate the trade secret; has possession of the trade secret; the application describes with reasonable particularity the matter to be seized and [reasonably] identifies the location where the matter is to be seized; the person against whom seizure would be

ordered would make such matter inaccessible to the court, if the applicant were to proceed on notice to such person; and, the applicant has not publicized the requested seizure." [16] The court order may also enjoin other associated devices or activities. *See id*. The original purpose of this remedy was to provide a means for the court to exercise their jurisdiction effectively in counterfeiting cases, i.e. to ensure the supposedly counterfeit goods were not destroyed before the trial started. [17] In regards to the DTSA, this is aimed at preserving the evidence and quickly hindering the misappropriation of the trade secret(s). [18]

II. Issues

The first issue is that currently most trade secret cases are of the "breach of confidentiality" type. [19] These would not require as extreme of a remedy as an off-site computer hacking activity would entail. Temporary restraining orders are sufficient in "breach of confidentiality" cases and the potential far-reaching effect of *ex parte* remedies could be quite damaging to our economy, particularly small businesses and start-ups. [20] Preventing the disclosure of trade secrets remains the number one priority and there is a strong argument for the need for the *ex parte* civil seizure remedy in special circumstances, for example espionage cases. The question then becomes is this specific remedy necessary for these supposed "worst-case" scenarios? Those against the DTSA have an answer for that, as well. They claim that these are the cases the EEA was originally designed to tackle. [21] The concern from the drafters of the DTSA is that federal prosecutors, with their power to obtain a search warrant, do not act quickly enough in these situations. [22] The DTSA dissenters believe that is due to the lack of merit in the majority of the claims. [23] In other words, is this a broad stroke remedy for a problem that is actually rather uncommon? It seems the answer depends on whom you ask. [24]

The serious issue the dissenters have with the *ex parte* remedy is that it would be the most significant tool a trade secret troll could employ. [25] The power of seizure could be rather easily used incorrectly in situations where information is mistakenly categorized as a trade secret. There is the potential for substantial policy issues in these circumstances, namely the effect this power would have, if used by trade secret trolls, on innovation and small businesses. [26] If the requirement threshold for the remedy is low, than small businesses and start-ups could have necessary components of their businesses, such as their computers and cell phones, seized on unsubstantiated claims. If the threshold is high, these cases may never make their way to the judge and would instead be determined in the marketplace.

Take the following example. Imagine a small business or start-up receives a letter from a trade secret troll that threatens seizure and legal action. The business will have to make a decision at that moment in time as to whether it has the resources for litigation. If it does, it will spend money and time in the courtroom to rid itself of the trade secret troll. If it does not have the resources and time, it will have to most likely compensate the trade secret troll with a monetary settlement. Either way the trade secret troll has drastically altered these small businesses or start-ups based on an unproven accusation. Trolls do not worry about the merits of their case; they are focused on threats of litigation and early settlements. Once again we are left with a question of whether the remedy designed to address the problem of espionage, likely foreign, is worth the possible disruption it could cause United States businesses and their innovation. Detractors of the DTSA do not believe so.

It is without a doubt that United States companies are facing a new and complex threat of cyber espionage. Look no further than the continuing fallout from the Sony Entertainment situation

and the seemingly constant state-backed foreign hacking attempts to countless other United States companies. [27] The importance regarding the law surrounding trade secrets cannot be questioned either.

CONCLUSION

A vital part of our economy, start-ups and small domestic businesses, could be significantly disrupted and irreparably harmed by our solution to these novel cyber espionage threats. Trade secret trolls have ceased to exist because of the current structure of trade secrets law. Protecting trade secrets is the fundamental aspect that both parties are concerned with. It would be fair to say that the detractors of the Defend Trade Secrets Act are not necessarily opposed to legislation to establish a federal civil cause of action for trade secret misappropriation. The important distinction is to make certain there are adequate safeguards against improper and putative use of such legislation. The detractors are clearly not convinced the Defend Trade Secrets Act sets in place those necessary safeguards and, without those, the arrival of trade secret trolls could be on the very near horizon.

SOURCES

[1]. “Trade Secret," *Legal Information Institute*, (28 Oct. 2015), https://www.law.cornell.edu/wex/trade_secret.

[2]. *Id.*

[3]. *Id.*

[4]. David S. Levine & Sharon K. Sandeen, *Here Come the Trade Secret Trolls*, 71 Wash. & Lee L. Rev. 230, 235-37 (2015).

[5]. *Id.*

[6]. *Id.*

[7]. *See id.*

[8]. *Latest Updates on Federal Trade Secrets Legislation*, Trading Secrets, (28 Oct. 2015), http://www.tradesecretslaw.com/latest-update-on-federal-trade-secret-legislation/.

[9]. *Senate, House Leaders Introduce Bipartisan, Bicameral Bill to Protect Trade Secrets*, US Senator Orrin Hatch, (July 29, 2015), http://www.hatch.senate.gov/public/index.cfm/releases?ID=ad28f305-f73a-4529-84ba-ad3285b09d6e.

[10]. *Id.*

[11]. *Id.*

[12]. Levine & Sandeen, *supra* at 245.

[13]. *Id.*

[14]. *Id*., *Latest Updates on Federal Trade Secrets Legislation*, Trading Secrets, (October 28, 2015), http://www.tradesecretslaw.com/latest-update-on-federal-trade-secret-legislation/.

[15]. See *Latest Updates on Federal Trade Secrets Legislation*, Trading Secrets, (October 28, 2015), http://www.tradesecretslaw.com/latest-update-on-federal-trade-secret-legislation/.

[16]. H.R. 3326, 114th Cong. 1st Sess. (2015).

[17]. Lisa Pearson, et al.*, An Overview of Legal Remedies Against the Trafficking in Goods Bearing Counterfeit Trademarks and Gray Market Goods Under United States Law*, Intellectual

Property Desk Reference, http://www.kilpatricktownsend.com/~/media/Files/articles/LPearsonOverviewofLegalRemedies.ashx.

[18] *Id*.

[19] Levine & Sandeen, *supra* at 253.

[20] *Id.* at 252-53.

[21] *Id*. at 254.

[22] *Id.* at 258.

[23] *Id.*

[24] *Latest Updates on Federal Trade Secrets Legislation*, Trading Secrets, (28 Oct. 2015), http://www.tradesecretslaw.com/latest-update-on-federal-trade-secret-legislation/.

[25] *See* Levine & Sandeen, *supra* at 256.

[26] See *id.* at 256-57.

[27] *Sony To Pay Out $3.5M To Lawyers To Settle Hacking Class Action Suit*, Deadline, (October 20, 2015), http://www.deadline.com/2015/10/sony-to-pay-out-3-5m-to-lawyer-to-settle-hacking-class-action-suit-1201588666/, *Is China Still Hacking US? This Cyber Firm Says Yes*, CNBC, (October 19, 2015), http://www.cnbc.com/2015/10/19/china-hacking-us-companies-for-secrets-despite-cyber-pact-.html.