Washington and Lee Law Review Online

Volume 71 | Issue 4 Article 3

1-21-2015

Here Come the Trade Secret Trolls

David S. Levine
Elon University School of Law

Sharon K. Sandeen
Hamline University School of Law

Here Come the Trade Secret Trolls

David S. Levine and Sharon K. Sandeen*

Abstract

Within the past few years, the U.S. federal government has been forced to confront the massive but hard-to-quantify problem of foreign and state-sponsored cyberespionage against U.S. corporations, from Boeing to small technology start-ups, and (as of this writing) perhaps Sony Pictures Entertainment. As part of that effort, Congress has taken up the Defend Trade Secrets Act and the Trade Secret Protection Act, which would create a private cause of action under the federal Economic Espionage Act. This Article addresses the possibility of introducing trolling behavior—using litigation as a means to extract settlement payments from unsuspecting defendants—to trade secret law through creation of a federal private trade secret misappropriation cause of action. Like the existing problem of patent trolls, trade secret trolling has the potential to undermine the structure of trade secret law and create serious problems and costs for innovators across all industries. Thus, this Article addresses the heretofore unexplored link between patent and trade secret trolling established by this legislation. It assesses in detail the benefits and downsides of creation of a federal trade secret misappropriation cause of action and, for the first time, the risk of trolling.

---

* David S. Levine is a Visiting Research Collaborator at the Center for Information Technology Policy at Princeton University, Affiliate Scholar at the Center for Internet and Society at Stanford Law School, and an Associate Professor at Elon University School of Law. Sharon K. Sandeen is a Professor at Hamline University School of Law and the author (with E. Rowe) of the leading casebook on trade secret law and *Trade Secret Law in a Nutshell*, both published by West Academic. The authors thank Daniel Lawall and Courtney Pine for their research assistance, and the editors and staff of the Washington and Lee Law Review for their thorough and expeditious work. Any errors and opinions expressed are those of the authors.

Table of Contents

I. Introduction

For several years, the bane of the existence of innovators has been the possibility of being attacked by the "patent trolls," also alternatively known as "non-practicing entities" or "patent assertion entities."[1] Concerned legislators have focused on

1. "Patent troll" is the popular name for "patent assertion entity" (PAE), defined as an "entity that uses patents primarily to obtain license fees rather than to support the development or transfer of technology." COLLEEN V. CHIEN, PATENT ASSERTION ENTITIES 4 (2012), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2187314 (describing PAEs in

deterring trolling activity in the patent space since the passage of the America Invents Act.[2] There is a wide-ranging consensus, if not unanimity, that trolling has been a significant drain on innovation.[3]

Trade secrecy has been generally free of similar trolling behavior, but two bills introduced in the last Congress, and the general perspective on trade secret law and practice that they reflect, could disturb that relative peace. The bills, the Defend Trade Secrets Act of 2014[4] (DTSA) and the Trade Secret Protection Act of 2014[5] (TSPA) (collectively, the Acts), likely to be reintroduced in the early part of 2015,[6] would create a new

---

a DOJ/FTC hearing on December 12, 2012). PAEs "make it economical to bring suit, and economical for the defendant to settle, regardless of the merits." *Id.* at 18–19. Thus, it should be no surprise that PAEs brought 61% of all patent infringement lawsuits from January 1 through December 10, 2012. *Id.* at 23. The potential trolling here is the hyper-aggressive use of alleged trade secret status to intimidate, vex, and exact settlements, not the acquisition of trade secret rights for the sole purpose of litigation. In that way, trade secret trolls may exhibit the same tactical behavior as patent trolls even as their alleged rights acquisition may differ.

2. Pub. L. No. 112-29, 125 Stat. 284 (2011) (codified at 35 U.S.C. §§ 100–212 (2012)).

3. Getting a handle on all of the impacts is a challenge. *See* CHIEN, *supra* note 1. The White House has explained that "PAE activities hurt firms of all sizes. Although many significant settlements are from large companies, the majority of PAE suits target small and inventor-driven companies. In addition, PAEs are increasingly targeting end users of products, including many small businesses." EXEC. OFFICE OF THE PRESIDENT, PATENT ASSERTION AND U.S. INNOVATION 1 (2013), http://www.whitehouse.gov/sites/default/files/docs/patent_report.pdf.

4. S. 2267, 113th Cong. (2014).

5. H.R. 5233, 113th Cong. (2014).

6. See Randall E. Kahnke et al., *Top 10 Trade Secrets Developments of 2014: Part 1*, LAW360.COM (Dec. 16, 2014, 10:00 AM), http://www.law360.com/articles/603592/top-10-trade-secrets-developments-of-2014-part-1 (last visited Jan. 11, 2015) ("Although it is uncertain whether further action will be taken as the current congressional term winds down, momentum is clearly building and a federal trade secret law may be on the horizon.") (on file with the Washington and Lee Law Review); David R. Pruitt, *Will Congress Enact a Federal Trade Secrets Act in 2015?*, NAT'L L. REV. (Dec. 12, 2014), http://www.natlawreview.com/article/will-congress-enact-federal-trade-secrets-act-2015 (last visited Jan. 11, 2015) ("The House's Trade Secrets Protection Act and the Senate's Defend Trade Secrets Act are likely to be considered in early 2015.") (on file with the Washington and Lee Law Review).

private cause of action under the Economic Espionage Act of 1996[7] (EEA) with the commendable purpose of addressing the problem of cyberespionage.[8]

As recent high-profile incidents reveal,[9] U.S. companies face significant threats from those who would hack into their computer systems, including operatives of foreign governments, organized crime syndicates, and various nuisance hackers and thrill-seekers.[10] Evidence even suggests that some governments are specifically initiating and supporting theft of U.S. trade secrets from private companies via unauthorized intrusions into computer networks as a means to further their own economic development.[11] Other high-profile intrusions, like the recent unauthorized disclosure of vast quantities of information from Sony Pictures Entertainment's computer network, remain shrouded in mystery; was the intrusion the act of a foreign government, or an inside job?[12] Regardless of the perpetrators, the Acts purport to address these and other misappropriations that occur via the use of the Internet and other digital technology.

Senator Christopher Coons (D-DE), one of the DTSA sponsors, stated that the Acts are intended to address the pervasiveness of foreign cyberespionage. As a press release from his office explains:

> In today's electronic age, 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. These losses put U.S. jobs at risk and threaten incentives for

---

7. Pub. L. No. 94-12, 110 Stat. 3488 (1996) (codified in scattered sections of 18 U.S.C. and 42 U.S.C.).

8. *See* 18 U.S.C. § 1831 (2012) (prohibiting economic espionage).

9. *See, e.g.*, MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 2 (2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (discussing several major cyberattacks by a Chinese hacking organization).

10. *Id*.

11. *Id.* at 1 (quoting U.S. Representative Mike Rogers, Oct. 2011).

12. *See generally Sony Pictures Hackers 'Got Sloppy', FBI Says*, BBC NEWS (Jan. 7, 2015, 3:51 PM), http://www.bbc.com/news/technology-30720003 (last visited Jan. 18, 2015) (discussing speculation on the source of the cyberattack on Sony) (on file with the Washington and Lee Law Review).

> continued investment in research and development. Current federal criminal law is insufficient.[13]

However, the Acts do not address, much less solve, these very real concerns. Instead, as this Article explains, the Acts are 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. By initiating lawsuits designed only to extract settlement payments or massive damage awards from scared defendants, trade secret trolls could cause the same drag on innovation and job growth that has been the hallmark criticism of the well-known "patent troll." Indeed, as acquiring trade secret status and initiating trade secret lawsuits—which can include separate claims involving covenants not to compete, nondisclosure agreements, and labor mobility—are significantly less expensive and time-consuming than similar activity in the patent space, the relatively low barriers to trolling suggests that this activity could be very widespread. At any rate, the potential for trolling behavior is rather obvious.

The Acts give rise to trade secret trolls by threatening to undermine decades of trade secret law and policy. Combined with an extraordinary power to seize a defendant's assets prior to judgment, these dangerous Acts incentivize trolling without doing much of anything for victims of cyberespionage. Thus, this Article explains the risk of trade secret trolling by expanding upon the Acts' previously identified infirmities and downsides[14] to explain the scope of the potential problem and assess alternatives that would not spur trolling but would still address cyberespionage. To

---

13. Press Release, Office of Senator Christopher Coons, Senators Coons, Hatch Introduce Bill to Combat Theft of Trade Secrets and Protect Jobs (April 29, 2014), http://www.coons.senate.gov/newsroom/releases/release/senators-coons-hatch-introduce-bill-to-combat-theft-of-trade-secrets-and-protect-jobs (last visited Jan. 11, 2015) (on file with the Washington and Lee Law Review).

14. *See* David Levine & Sharon K. Sandeen, *Professors' Letter in Opposition to the "Defend Trade Secrets Act of 2014" (S. 2267) and the "Trade Secrets Protection Act of 2014" (H.R. 5233*), CTR. FOR INTERNET & SOC. (Aug. 26, 2014), http://cyberlaw.stanford.edu/files/blogs/FINAL%20Professors%27%20Letter%20Opposing%20Trade%20Secret%20Legislation.pdf (hereinafter *Professors' Letter*) (urging Congress to reject the Acts on behalf of thirty-one U.S. professors).

be sure, the capabilities of trade secret trolls remain to be seen, but the risk is very real.

To many, the trade-secret-troll threat born out of the Acts may not be readily obvious, primarily because the rhetoric surrounding the Acts focuses on the putative trade secret owner (i.e., the plaintiff) instead of the equally important businesses, including many start-ups, that may be wrongfully accused of trade secret misappropriation (i.e., the defendant). In other words, the Acts appear to enshrine trade secrecy exclusively within the realm of property theory, despite the fact that the Acts are putatively designed to address the torts of unauthorized intrusions into computer and corporate networks.

To see the threat caused by the Acts requires an understanding of how the two primary theories of trade secret law work in tandem to create nuanced law that appropriately balances the prevention of bad acts with the benefits of free competition, information diffusion, and employee mobility. While tort-based concepts of improper acts and wrongful conduct by individuals and entities pervade trade secret law, a claim of trade secret misappropriation requires more than just an improper act. It also requires the actionable form of property colloquially called a "trade secret." The existence of this property interest, when acting in concert with the tort rationale, operates to check the excesses of sole application of either theory. Thus, when an entity takes something through an improper act that is not a trade secret, it is not a trade secret misappropriation.

The Acts and the rhetoric surrounding them fail to appreciate this seemingly obvious point. As a consequence, many of the bad acts that Congress seeks to prevent will not be addressed due to the absence of legitimate trade secrets. In other words, focusing exclusively on protecting perceived trade secret rights misses the point that what we really care about is preventing certain behaviors that are deemed wrongful (such as unauthorized computer hacking).

Ironically, such is the historical purpose of tort law. In this instance, however, the hyper-focus on property rights has led Congress astray by creating a proposed tort that focuses more on alleged property rights than on bad behaviors. Thus, to see the threats posed by the Acts requires an understanding that not all

business information, and not even all secret information, has a property right of protection through trade secret law.

Exacerbating the risks of passing the Acts is the fact that businesses often believe that they own trade secrets when they do not and attempt legal actions on alleged misappropriations of information unworthy of protection due to their suspect secrecy status. The narrow theoretical orientation reflected in the Acts has apparently blinded proponents of the Acts to that reality, as well as the harms identified and critiqued in this Article. Instead, this Article approaches trade secrecy from the more appropriate theoretical perspective of trade secrecy as a tort-based concept focused on wrongful acts, like cyberespionage, rather than tied to property and ownership.

Additionally, seeing the threat requires an appreciation for the important and historical values of labor mobility and the diffusion and sharing of knowledge and information that underlie U.S. economic development. One of the reasons trade secret law does not involve exclusive property rights is because those values need to be balanced against the protection of trade secrets.[15] Unfortunately, the Acts ignore all but property values while reinforcing misunderstandings and misconceptions about the role of trade secrecy in innovation theory and policy. Instead of clarifying the law, they muddy the waters. Rather than addressing cyberespionage, the Acts point to one result: the advent of the trade secret troll, a beast borne of information control rather than diffusion.

This Article discusses, in Part II, the factual and theoretical predicates of the Acts and their ramifications for the birth and expansion of trade secret trolls. Through discussion of the threat of the yet-unknown trade secret troll, it also frames the discussion about trade secrecy around information diffusion and the tort of misappropriation, rather than the problematic focus on property rights and ownership. In that way, the Article steers the discussion about trade secrecy away from the property-centric

15. *See id.* at 4 ("A hallmark of all US intellectual property laws, including trade secret law, is that they include limiting doctrines that are designed to achieve the appropriate balance between the protection of intellectual property rights and the preservation of free competition.").

focus usually applied to tort-like thefts, about which innovators and policymakers are rightly concerned, and toward its traditional grounding in unfair competition law. Built upon this reorientation, Part III suggests alternatives to the Acts in addressing the threat of cyberespionage, primarily by amending the Computer Fraud and Abuse Act.[16]

II. Factual Predicates and the Troll

To understand the threat of trolling—and, therefore, how trade secret trolls could emerge—requires an appreciation of the current state of trade secret law, developed in this Article by examination of five of the core factual predicates in favor of the Acts. Proponents of the Acts proffer these factual predicates with little critical analysis.[17] Accepting the following factual predicates as asserted would foster an environment where trade secret trolls might flourish.

The failure to adequately explore these factual predicates has been a clarion call that this Article seeks to correct. In that way, this Article seeks to engender a more granular understanding of the theory and practice of trade secret law for a modern, porous, and technologically-infused economy and society. The need for this analysis transcends the Acts, as trade secrecy is on the rise both as a commercial practice and a source of litigation. Thus, scholars and policymakers should apply the assessment and concern about incentivizing trade secret trolls described below to any future efforts to alter trade secret law at the state or federal level.

---

16. 18 U.S.C. § 1030 (2012).

17. There have been two significant critical articles written about trade secret law reform, both opposed. *See* Zoe Argento, *Killing the Golden Goose: The Dangers of Strengthening Domestic Trade Secret Rights in Response to Cyber-Misappropriation*, 16 YALE J.L. & TECH. 172 (2014); Christopher Seaman, *The Case Against Federalizing Trade Secrecy*, 101 VA. L. REV. (forthcoming 2015), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2397567.

A. Harms: "We Know What We Need to Know to Pass the Acts."

A principal premise of the proposed legislation is that billions of dollars of U.S. trade secrets have been misappropriated in recent years and that trade secret holders need federal legislation to solve this problem.[18] However, getting a fix on exactly how much information, let alone how many actual trade secrets, is being misappropriated and by whom is a difficult task, leading to a dearth of reliable data. Nor can the threat to trade secrets as a result of cyberespionage be accurately measured. As John Villasenor recently explained, it is "impossible to know how many trade secret misappropriation incidents are tied to cybersecurity breaches."[19] While Villasenor concedes that "there is good reason to believe that many of them are,"[20] it is a fool's errand to attempt to create a complex new federal cause of action under such uncertainty, as the likelihood of making things worse is at least as great as the chance of improvement. The certainty, if any, is that the Acts will do more harm than good.

The aforementioned breach of Sony's computer network provides a case in point. Although state-sponsored cyber-espionage was suspected initially,[21] experts in hacking have recently opined that the data breach was the result of a rogue employee(s) who, apparently, had legitimate access to Sony Picture's stored data for years.[22] If so, this event is an example of

---

18. *See* Argento, *supra* note 17, at 174–76 (discussing background for introduction of trade secret legislation); Seaman, *supra* note 17, at 4–5 (noting that "intellectual property theft is estimated to cost U.S. firms billions of dollars annually").

19. John Villasenor, *Corporate Cybersecurity Realism, Managing Trade Secrets in a World of Where Breaches Occur* 9, 43 AIPLA Q.J. (forthcoming 2015)*, available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2488756.

20. *Id.*

21. *See* Michael S. Schmidt et al., *F.B.I. Says Little Doubt North Korea Hit Sony*, N.Y. TIMES (Jan. 7, 2015), http://www.nytimes.com/2015/01/08/business/chief-says-fbi-has-no-doubt-that-north-korea-attacked-sony.html?_r=0 (last visited Jan. 18, 2015) (on file with the Washington and Lee Law Review).

22. *See* Dana Liebelson, *Ex-Sony Employees Echo Cybersecurity Company's Suspicion That Hack Was An Inside Job*, HUFFINGTON POST (Jan. 7, 2015, 12:59 AM), http://www.huffingtonpost.com/2015/01/06/sony-hack_n_6425262.html (last visited Jan. 18, 2015) (on file with the Washington and Lee Law Review).

information disclosure by employees that is already actionable under existing trade secret law, rather than a new form of wrongdoing that needs a new federal cause of action. Alternatively, if this was a hack orchestrated by the North Korean government, then utilizing trade secret law will assuredly not be an effective remedial route for Sony.[23] Moreover, it appears that much of the information that was allegedly hacked would not qualify for trade secret protection, rendering trade secret law utterly irrelevant to the issue. And yet, we can expect that the Sony example will be used to justify the need for the Acts.

Another reason for the dearth of reliable data is the aforementioned lack of understanding of trade secrecy's nuances. The methodology used to collect loss statistics is often based upon surveys by business executives who do not understand the scope and limits of trade secret law—specifically, the definition of a trade secret and of misappropriation.[24] Without knowledge of the intricacies of trade secret law, claims of trade secrets loss tend to be overstated because the responses to the surveys are more likely based upon the layperson's definition of a trade secret, which, unlike the legal definition, usually includes any information that a business keeps secret. Similarly, many business executives may not be aware that reverse engineering is a proper means of acquiring trade secrets or that the value of trade secret information, if any, must derive directly from its secrecy. Also, the surveys do not typically ask whether the respondents have been sued for trade secret misappropriation and how much they had to spend to defend illegitimate claims, costs that should be balanced against the asserted benefits of the Acts.

We also have inaccurate data concerning the source of threats to trade secrets and the magnitude of the threat of foreign espionage.[25] The existing data establishes that the bulk of all

---

23. For a potential framework to address this problem, see Lawrence J. Muir, Jr., *Combatting Cyber-Attacks Through National Interest Diplomacy: A Trilateral Treaty with Teeth*, 71 WASH. & LEE L. REV. ONLINE 73 (2014).

24. *See* Villasenor, *supra* note 19, at 10 (noting the difficulty in putting a number on trade secret and cybersecurity losses).

25. *See id.* at 10–11 (discussing the known, and unknown, threats to trade secrets and cybersecurity). Even if we assume that there are significant threats

trade secret cases are of the domestic variety, typically involving alleged breaches of confidence in the context of business-to-business and employer–employee relationships.[26] Trade secret cases based upon the alleged acquisition of trade secrets by espionage and other improper means are much fewer in number. Moreover, there is no data to support the assertion that the Department of Justice (DOJ) is unwilling or unable to prosecute the handful of cases annually that involve foreign espionage.[27]

Despite the foregoing, even assuming (as we do) that trade secret misappropriation is a significant problem that requires a remedy, the United States already has a robust body of civil and criminal trade secret law that currently provides the most stringent protection in the world.[28] Thus, it is unclear how limited statistics justify the adoption of a federal civil cause of action. Indeed, according to the recently updated Organization for Economic Cooperation and Development Trade Secret Protection Index, the current trade secret protection system of the United States ranked highest among the countries studied, receiving 4.5 out a possible 5 points.[29] This establishes—with as good a data set as we might currently find—that the current system is already doing great work protecting the trade secrets of U.S. businesses.

The dearth of data, combined with a widely held but unsubstantiated belief that a federal private cause of action would help, will not help to address, much less solve, the

---

of espionage from individuals who are located outside of the United States despite the existence of meaningful data, the Acts do not even begin to address those threats, as the proposed legislation does not have any extraterritorial effect outside of the United States. *See infra* Part II.B.

26. *See* David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in State Courts*, 46 GONZ. L. REV. 57, 59–60 (2011); David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 GONZ. L. REV. 291, 303 (2010).

27. These allegations remain unsupported, especially as the DOJ may work with private industry in ways that do not result in prosecution, but rather support (i.e., assistance in conducting investigations). *See infra* Part II.C.

28. *See Professors' Letter*, *supra* note 14, at 2 (discussing existing state and federal law).

29. ORG. FOR ECON. COOPERATION & DEV., PROTECTION OF TRADE SECRETS 2 (2014), http://www.oecd.org/trade/tradedev/OECD-tad-protection-of-trade-secrets-web-annotation.pdf.

unquantified problem of cyberespionage. Rather, a federal civil cause of action for trade secret misappropriation is far more likely to be wielded by those who seek to exact rents from the unwary and utilize litigation as a method of competitive destruction rather than innovation.[30] Thus, it portends the creation of the "trade secret troll" because there is a significant risk that a new federal civil cause of action for trade secret misappropriation will be used too aggressively by those who think they own trade secrets when, in many situations, all they own is information that they think is valuable or, as in the case of Sony Pictures, embarrassing. Until now, this eventuality has not even been considered, much less analyzed, but it appears to be a far more certain outcome than any other.

To avoid the creation of trade secret trolls, detailed public hearings are needed. These hearings must focus on the range of interests at stake, from small businesses for whom litigation is a difficult or impossible financial burden, to civil society that wants access to trade secret information, to trade secret defendants, and to the federal judiciary that will necessarily be called upon to hear more cases. Congress must scrutinize the existing data for evidence that might support or undermine the assumptions baked into the Acts—namely, that foreign cyberespionage requires a federal private remedy. Policymakers should then balance this evidence against the costs of a new federal claim for relief, including the potential misuse of trade secret misappropriation claims to disrupt competition and quell employee mobility. In other words, the risk of trade secret trolling must be part of the discussion.

Especially when compared to the many recent hearings involving copyright and patent reform,[31] the Acts have received

---

30. *See Professors' Letter*, *supra* note 14, at 3–4.

31. *See Congressional Hearings on the Review of the Copyright Law 2014*, U.S. COPYRIGHT OFF., http://copyright.gov/laws/hearings/ (last visited Jan. 11, 2015) (listing eleven separate hearings in 2014 held by the House Judiciary Committee's Subcommittee on Courts, Intellectual Property, and the Internet on copyright reform) (on file with the Washington and Lee Law Review); *Testimony and Statements*, AIPLA, http://www.aipla.org/advocacy/congress/Pages/Testimony.aspx (last visited Jan. 11, 2015) (listing a litany of letters and testimony offered to Congress over the past few years, most of which concern patent law) (on file with the Washington

virtually no critical attention and have yet to be the subject of any robust public hearings. Although public hearings have been held concerning the problem of cyberespionage,[32] almost all attention has been paid to the voices of large corporations and their lobbyists who have focused exclusively (and naturally) on the threats to their valuable information. To be sure, this is an important concern that most agree needs to be addressed more thoroughly. However, there is another side to this issue—that of the defendants in trade secret cases, many of whom are the individuals and businesses that our intellectual property law policy purports to encourage.

The voices of talented individuals who simply wanted to progress in their careers by switching jobs, only to be sued for trade secret misappropriation, have not been heard. Nor have the voices of entrepreneurs and small businesses that had an idea for a better product or service but found themselves in the midst of trade secret litigation because they hired talented people from a competitor company. Or, for that matter, any defendant who found itself on the wrong side of an aggressive trade secret plaintiff whose tactics, regardless of the merits of the dispute, caused it economic harm. The assertion of unfounded trade secret claims are torts in and of themselves that warrant discussion and evaluation in future hearings around the Acts.

It is axiomatic that law must be based on the best information that can be adduced from the range of legitimate interests that exist within a policy area. Congress has not yet begun to gather that information. Thus, before Congress creates a new avenue into federal courts for trade secret plaintiffs, it should have a clear understanding of the impact, costs, benefits, and ramifications of such a path on trade secret defendants. Therefore, the voices of those who may be victimized by a putative trade secret troll's aggressive litigation tactics, and perhaps more significantly, threats of litigation, must be shared

---

and Lee Law Review).

32. *See, e.g.*, *Cyber Espionage and the Theft of U.S. Intellectual Property and Technology: Hearing Before the H. Subcomm. on Oversight and Investigations*, 113th Cong. (2013), http://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/Hearings/ OI/20130709/HHRG-113-IF02-MState-M001151-20130709.pdf.

with policymakers in the same settings that have been afforded large corporations and their lobbyists. Enacting the Acts without the hearings and debate is a surefire way to create the unintended harms associated with trade secret trolls.

B. Law: "The Acts Create Uniformity Because Current U.S. Trade Secret Law Lacks It."

Another argument for the Acts suggests that the purported lack of uniformity in state trade secret law makes enforcement of trade secret rights time-consuming, slow, and resource-intensive.[33] Meanwhile, so the argument goes, trade secrets are being ferried out of the United States. However, the assertion that U.S. trade secret law is not substantially uniform is incorrect and misleading, particularly with respect to the key definitions of a "trade secret" and "misappropriation."[34] The assertion is also inconsistent with representations that the United States has made to the World Trade Organization regarding U.S. compliance with Article 39.2 of the TRIPS Agreement.[35] This factual predicate primarily benefits trade secret trolls to the extent that it is believed, but it is simply not true.

The fact is that U.S. trade secret law is very uniform due to the widespread adoption of the Uniform Trade Secrets Act (UTSA). The definitions of a trade secret and of misappropriation that apply in forty-seven states are the UTSA definitions (with some minor but insignificant differences in some states).[36] These definitions, in turn, are consistent with both the language of

---

33. *See* Seaman, *supra* note 17, at 35 n.240 (discussing proposed benefits of the Acts).

34. *See id*. at 43 n.296 (noting that "the Federal Circuit has acknowledged [that] 'trade secrets law varies little from state to state'" (quoting TianRui Grp. Ltd. v. Int'l Trade Comm'n, 661 F.3d 1322, 1327–28 (Fed. Cir. 2011))).

35. *See* Agreement on Trade-Related Aspects of Intellectual Property Rights art. 63.2, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299; *see also* First Submission of the United States, *United States—Main Dedicated Intellectual Property Laws and Regulations*, Table AIII.4, IP/N/1/USA/1 (Jan. 20, 1996) (listing applicable state law).

36. *See* Seaman, *supra* note 17, at 36 (discussing the widespread adoption of the UTSA).

Article 39.2 of the TRIPS Agreement and the existing Economic Espionage Act because the UTSA definition was used as the model in both instances. In the three states that have yet to adopt the UTSA (North Carolina, New York, and Massachusetts), both applicable statutes and case law define a "trade secret" and "misappropriation" in ways that are generally consistent with the UTSA definition.[37] So from where does this argument derive?

Sometimes the perceived lack of uniformity is based upon a failure to appreciate the effect of other principles of law on the application of trade secret principles. Trade secret law, having been developed at common law in the United States, is closely tied to other areas of state law that, depending upon the case, a court will apply in trade secret litigation.[38] Among these laws are common law and statutory principles of employment law, duties of confidence, antitrust law, unfair competition law, and civil procedure. Thus, when people complain of a lack of uniformity in trade secret law, it is often because of the application of these other areas of law and is not a result of a lack of uniformity of trade secret doctrine.[39]

Significantly, the Acts do not address these ancillary legal doctrines; nor could they, given the fact that these doctrines often reflect the values and interests of individual states. More importantly, many of these state laws operate to prevent trade secret claims from being used as anti-competitive weapons and are, therefore, important constraints on the emergence of trade secret trolls. In other words, entrepreneurial individuals and start-up companies often benefit from the space that these doctrines create to legally compete and maneuver. They also provide the critical "balance" between legal and illegal behavior that all intellectual property laws in the United States are supposed to have. Their absence in the Acts herald the emergence

---

37. *See* Argento, *supra* note 17, at 178 (discussing the holdout states); Seaman, *supra* note 17, at 36 (discussing the three holdout states).

38. *See* Seaman, *supra* note 17, at 48 (discussing the interrelated nature of trade secret claims and other areas of state law).

39. *See id.* at 47 n.325 (noting that "even 'under a federal trade secret statute, trade secret owners would likely be faced with geographic differences in the case law interpreting that statute'" (quoting AM. INTELLECTUAL PROP. LAW ASS'N, REPORT OF THE AIPLA TRADE SECRETS COMMITTEE (2007))).

of trade secret trolls who will thrive in a plaintiff-friendly space built on the principle of empowering those on the litigation offensive. Use of the Acts will undoubtedly move well beyond the cyberespionage situations that they are intended to address.

The argument that U.S. trade secret law is not uniform also evinces a lack of understanding of the practical significance of minor differences in the UTSA as adopted by a handful of states.[40] More often than not, these differences involve procedural issues, such as the applicable statute of limitations or the burden of proof on some issues. In the few states where the definition of a trade secret differs from the UTSA definition, the difference is usually because the statute adds to the litany of things that can be a trade secret without really changing the uniform definition (which is very broad without an expanded litany). Efficient administration of justice and commerce in the U.S. relies heavily upon scores of uniform laws (including the Uniform Commercial Code) that, as adopted by the various states, are not precisely uniform. Thus, to use the asserted lack of uniformity in U.S. trade secret law as a justification for the Acts would set a terrible precedent and could undermine federalism by justifying federal legislation in areas that have long been the province of the states.

Trade secret owners often perceive a lack of uniformity in trade secret law because of the fact-specific nature of trade secret claims and the fleeting nature of trade secret rights.[41] As noted previously, a business will oftentimes believe that it owns valuable trade secret information when, in fact, it does not. This can happen because information can cease being a trade secret through proper disclosures of the information by others. Indeed, under well-established trade secret doctrine, information can stop being a trade secret due to no actions or fault of the trade secret owner. This reality explains why a trade secret plaintiff may win a case in one state in year one and lose a similar case in another state in year two. Thus, we should not mistake the failure of a

---

40. *See, e.g.*, David S. Almeling, *Four Reasons to Enact a Federal Trade Secrets Act*, 19 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 769, 779 (2009) (discussing the benefits of creating a federal trade secret law, even if differences between states are small).

41. *See* Seaman, *supra* note 17, at 47 (discussing "fact-specific decisionmaking").

plaintiff in a trade secret case to prove its case by a preponderance of the evidence with a lack of uniformity. Instead, it should be viewed as the proper policing of what is and is not a trade secret.

The Acts will set the stage for the emergence of trade secret trolls by enshrining less uniformity, not more, into trade secret law,[42] and by eliminating essential checks against plaintiff abuse of power. Underscoring this point, the fact that the Acts have a statute of limitations that is two years longer than that set forth in the UTSA creates disunity on its face.[43] We should fully expect federal lawsuits after the time a state claim for relief has expired, a wonderful point of leverage for the trade secret troll. That leverage would allow for trade secret trolls to exact payments from defendants even as state courts have washed their hands of a dispute and potentially beyond the actual life of the trade secret.

Moreover, as a practical matter, longer statutes of limitations maintain uncertainty and unpredictability about legal exposure that can stall innovation and progress. In the case of trade secret misappropriation, the greater the uncertainty that the law creates with respect to a potential trade secret misappropriation claim, the less likely that we will see the benefits of protecting trade secrets, like innovation and job growth. As many trade secrets do not last very long anyway, it seems reasonable to require trade secret owners to act quickly or lose their rights to bring a lawsuit because the alternative scenario of quelling competition and entrepreneurship is much worse.

Several hypothetical questions illustrate how the very passage of the Acts could create less uniformity. When federal judges hearing cases under the new law encounter an issue (such as the definition of a duty of confidentiality or the meaning of "reasonable efforts") that is not addressed by the law, what law will they apply? Will they create federal jurisprudence to fill in the gaps or will they use legal principles of a state? If the latter, what if there is no consensus on various issues of state law, like

---

42. *See id.* at 43–48 (discussing various ways that federalization may result in less uniformity).

43. *See* UNIF. TRADE SECRETS ACT § 6 (1985).

application of the inevitable disclosure doctrine[44] and enforcement of noncompete agreements, both of which can be tools of hyper anti-competition? For instance, will they use Florida's view concerning the enforceability of noncompete agreements or California's view?[45]

Particularly while federal jurisprudence is developing to apply the new law, we should expect aggressive trolling to emerge while courts sort out what the Acts actually do and do not do and how to respond to their notable weaknesses. While the foregoing questions are sorted out, the trade secret troll will enjoy the unsettled terrain and perhaps succeed in keeping it unsettled for quite a while.[46] We need to ask whether this disruption of U.S.

---

44. There is currently a split among the states concerning whether the inevitable disclosure doctrine of U.S. trade secret law should be recognized or whether it amounts to an improper implied noncompete agreement. *Compare*, *e.g.*, PepsiCo, Inc. v. Redmond, 54 F.3d 1262 (7th Cir. 1995), *with* Whyte v. Schlage Lock Co., 101 Cal. App. 4th 1443 (2002).

45. Although most states in the United States find "reasonable" noncompete agreements enforceable if they are designed to protect a "legitimate business interest," there are significant differences of opinion among the states on the issues of: (1) what constitutes a legitimate business interest and (2) what restrictions are reasonable. Pursuant to a law dating back to 1872, California (arguably the most entrepreneurial state in the Union) takes the position that most noncompete agreements are void *ab initio* and that the use of such agreements to protect trade secrets is not a legitimate business purpose. *See* CAL. BUS. & PROF. CODE § 16600 (2014) ("Except as provided in this chapter, every contract by which anyone is restrained from engaging in a lawful profession, trade, or business of any kind is to that extent void."); Edwards v. Arthur Andersen, LLP, 189 P.3d 285 (Cal. 2008). Florida is among a handful of states that are on the other end of the continuum when it comes to the enforceability of noncompete agreements. Generally, they are presumed to be valid unless proven to be unreasonable. *See* FLA. STAT. § 542.335 (2014) ("[E]nforcement of contracts that restrict or prohibit competition during or after the term of restrictive covenants, so long as such contracts are reasonable in time, area, and line of business, is not prohibited.").

46. Another argument in favor of the Acts is that it will be easier to explain and understand U.S. trade secret law if there is a federal private cause of action. So the argument goes, it will be easier for U.S. negotiators to get other countries to agree to adopt trade secret law similar to U.S. law if it can be easily understood. If that argument is being weighed, it should be noted that to the extent that creating a federal private cause of action under the EEA is designed to be a negotiating tool in current ongoing, albeit secret, trade negotiations like the Transatlantic Trade and Investment Partnership, it may actually have the opposite effect of making U.S. law appear scattered rather than targeted. The United States' best argument for international adoption of trade secret

law is worth the marginal and speculative procedural benefits[47] that might result from a federal law versus a widely adopted uniform law.

C. Plaintiff's Story: "Without the Acts, It Is Difficult or Impossible to (a) Stop Fleeing Misappropriators, (b) Conduct Cross-Border Discovery, or (c) Enforce State Judgments in Cases Filed in State Court."

As best as the authors of this Article can tell, the most compelling factual scenario for the Acts is the first scenario above, the case of the fleeing misappropriating employee, particularly in multiple party cases when complete federal jurisdiction does not exist. The hypothetical (or reality) would be as follows: employee of company headquartered in state *A* plugs a thumb-drive into a computer and saves her employer's trade secrets to it. Employee leaves state *A* and heads immediately to an international airport in state *B*. Employer and fleeing employee have limited or no contacts with state *B*, making employer's willingness and ability to sue in state *B* questionable. Moreover, depending upon state *B*'s long-arm statute, acquisition of personal jurisdiction over the defendant may be difficult, and therefore the employer may not be able to interdict the fleeing employee in state *B* through state *B*'s courts. Federal law, so the argument goes, would allow for "national process" and the ability of the employer to more easily and quickly go into federal court in state *A* to prevent bad behavior in state *B*: to stop the rogue employee from getting on an airplane bound for a foreign country.

The foregoing story, while compelling, has factual holes. While it is undoubtedly a challenge to deal with a fleeing employee or multiple parties located in different states, court

---

principles and enforcement is the general success of our state-based innovation economy, which protects legitimate secrets while encouraging collaboration. While such a system could be improved, particularly on the access to information side, the Acts represent an unnecessary complication and bureaucratic layering rather than a solution. U.S. negotiators will have a much easier time explaining and justifying current U.S. trade secret law than explaining the muddied law that the Acts would spawn.

47. *See infra* Part II.C–E.

process, be it state or federal, is likely to be similarly cumbersome. Moreover, the magnitude of the problem (compared to all trade secret misappropriation claims) is not known. Given that many trade secret cases already land in federal court under diversity jurisdiction, the percentage of cases that could conceivably benefit from the Acts is significantly less than 100%. This is not only because some cases can already be filed in federal court based upon diversity jurisdiction, but because not all trade secret misappropriation cases would meet the "in commerce" requirements of the Acts.

Proponents of the Acts have not adequately explained exactly the scenario about which they are concerned nor what is lacking under the current trade secret regulatory system, which includes well-developed processes for cross-state litigation and border and criminal enforcement efforts. Indeed, the DOJ already has protocols in place to handle these scenarios successfully. In a 2009 U.S. Attorneys' Bulletin, an author discussed exactly this situation, wherein "law enforcement . . . learns that the defendant may have misappropriated trade secrets and is leaving the country in 48 hours or may be leaving the company imminently."[48] The DOJ identified a typical example of this behavior: "The defendant is at the airport and preparing to leave the country when an experienced U.S. Customs and Border Protection Officer notices something unusual and begins asking appropriate questions, revealing misappropriated trade secrets in the defendant's luggage or on the defendant's laptop."[49] Thus, the above is not a situation in which law enforcement lacks capacity and existing resources can prevent movement outside of the United States.

Noting that "prompt decisions concerning border searches typically are necessary,"[50] the Bulletin discusses law

48. Mark L. Krotoski, *Common Issues and Challenges in Prosecuting Trade Secret and Economic Espionage Act Cases*, U.S. ATTORNEYS' BULLETIN, Nov. 2009, at 2, 12, http://www.justice.gov/usao/eousa/foia_reading_room/usab5705.pdf.

49. *Id*. at 12 (citing United States v. Jin, No. 04-cr-20216 (N.D. Ill. Dec. 9, 2008)).

50. *Id.* at 13.

enforcement's ability to handle a scenario exceedingly similar to the primary scenario offered by the proponents of the Acts:

> Based on a tip, investigators learn of the misappropriation just before two defendants are boarding their international plane, requiring a decision on whether to arrest the defendants at the border. A search reveals that the defendants possess suspected trade secrets from four Silicon Valley companies, including technical schematics, information about design methodology, computer aided design (CAD) scripts, microprocessor specifications, and other technology information.[51]

These latter two stories are not hypotheticals, but examples of cases that actually arose. Thus, the DOJ has the expertise and experience to handle such scenarios. The real problem is that it can be difficult to discover trade secret misappropriation of this sort, but the Acts do nothing to address that problem.

Fortunately, contacting or tipping off law enforcement requires no court process and, if an actual threat exists, is undoubtedly a faster route to intercepting a rogue employee at an airport than attempting to get a court involved. Additionally, if the above scenarios include the element of surprise and the need for quick action, there will be nothing quicker than contacting law enforcement directly. In sum, it is unclear that the Acts would create a procedure that would be any quicker than that already in place. The law can do little to help companies prevent and detect trade secret misappropriation, which is a separate problem that we address below.

With regard to concerns about the costs of cross-border discovery and enforcement, they are true to a degree because applicable federal procedure is marginally more efficient than having to seek discovery and enforcement orders in more than one state. Nonetheless, cross-border discovery and enforcement, particularly among U.S. states, is not as difficult or costly as some suggest. There are existing procedures in place both within and outside of the United States (including applicable international agreements) that are currently used in all manner of civil and commercial litigation. But because the Acts will have only limited extraterritorial effect, they will not improve the

51. *Id*. (citing United States v. Fei Ye, 436 F.3d 1117 (9th Cir. 2006)).

existing conditions for international cross-border discovery and enforcement. In other words, while it is possible under existing language in the EEA to sue a U.S. citizen, a permanent resident alien, and even a foreigner in federal court for conduct occurring outside of the United States,[52] this provision of law does not address discovery and enforcement proceedings in another country at all.

Indeed, this factual predicate evinces a lack of understanding of the procedures that are currently available for the enforcement of foreign judgments and the conduct of transnational discovery (both among states and in foreign countries). Currently, forty-seven states have adopted the Uniform Enforcement of Foreign Judgments Act, which makes the enforcement of state judgments as easy as what currently exists between federal courts.[53] Essentially, the process requires the filing of an exemplified copy of the judgment with the appropriate court.[54] With respect to the enforcement of judgments in and from other countries, the process is admittedly more difficult, but the Acts do not even begin to address this problem, and Congress has shown little willingness to join existing international agreements concerning the enforcement of foreign judgments.

With respect to discovery, the Federal Rules of Civil Procedure do provide for greater ease of cross-border discovery than applicable state law procedures, but state law processes are routinely used by U.S. litigants and are not onerous. With respect to discovery in foreign countries, the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters[55] and the Inter-American Convention on Letters Rogatory[56] often apply to streamline the process, but, as with enforcement, the Acts do not directly address whatever discovery difficulties may apply in the rare trade secret cases that involve foreign defendants.

---

52. *See* 18 U.S.C. § 1837 (2012) (discussing EEA application to conduct occurring outside the United States).

53. *See generally* UNIF. ENFORCEMENT OF FOREIGN JUDGMENTS ACT (1964).

54. *See id.* § 2 (describing the effect of a judgment that has been filed with a court).

55. Mar. 18, 1970, U.S.T. 2555, 847 U.N.T.S. 241.

56. Apr. 15, 1980, S. TREATY DOC. NO. 98-27 (1984).

Finally, if the costs of cross-border litigation are a major concern of Congress, then that concern transcends trade secret law. But instead of approaching this purported problem holistically by aiding all commercial litigants, the Acts single out trade secrecy for special treatment without establishing the factual predicates for such exclusivity. Instead of solving the problems that exist, the Acts—at best and under very limited circumstances—create redundant procedures that are less effective against actual misappropriators than simply contacting law enforcement directly. Thus, the Acts would miss actual misappropriators but allow trade secret trolls to roam free in a confused and unsettled environment, threatening or initiating lawsuits for the sole purpose of exacting settlement payments, just like existing patent trolls.[57]

D. Asset Seizure: "Existing Seizure Provisions are Inadequate, Requiring the Acts' New Remedies."

Another argument in favor of a proposed federal civil right of action for trade secret misappropriation concerns the asserted need for a new "seizure" remedy to prevent spoliation of evidence and actual use of misappropriated trade secrets.[58] Once again, the need for this remedy is unsubstantiated and appears to be overstated. Instead, this broad seizure power, even with attempted checks against improper use, is likely to be the most potent weapon to be wielded, and abused, by the trade secret troll.

First, it is unclear from the language of the Acts why the existing power of state and federal courts to issue temporary restraining orders is not sufficient to protect the interests of deserving plaintiffs. Under applicable law governing the grant of temporary restraining orders and preliminary injunctions, courts already have broad discretion to order the seizure of information

---

57. *See* CHIEN, *supra note* 1, at 69 (noting that according to one study of patent trolls, "[b]ased on 900 litigations, in the majority of them, the legal costs exceed the settlement").

58. *See, e.g.*, Seaman, *supra* note 17, at 27–31 (describing the seizure remedy in the Acts).

and they are known to do so.[59] Additionally, if the destruction of evidence is the concern, there is already a considerable body of substantive and procedural law that prohibits the destruction of evidence, including federal criminal law,[60] similar state laws, rules of professional conduct, and the tort of spoliation of evidence.

It is also unclear exactly why and to what extent such a remedy is needed. The vast majority of trade secret cases are of the "breach of confidentiality" variety, involving individuals and companies in some sort of commercial or employment relationship and the voluntary disclosure of the trade secrets by the trade secret owner. In other words, many trade secret misappropriation claims do not involve the sort of off-site computer hacking activity that is a principal justification for the Acts. Moreover, having voluntarily shared its trade secrets, the trade secret owner (if it planned ahead) should have the power to control such usage and to secure necessary evidence from its employees—by reserving, for instance, the right to search company premises, requiring the return of company property, or engaging in timely exit interviews.

With respect to entity defendants (e.g., a new employer), it is standard practice for larger and more sophisticated companies to place a "legal hold" on documentary and digital information once the threat of litigation is known.[61] Therefore, particularly in employer/employee cases, it is likely that both the plaintiff and the defendant will have procedures in place to prevent the destruction of evidence. Moreover, while the actual destruction of information taken by a former employee may make it more difficult to prove the misappropriation, such destruction is beneficial to the trade secret owner to the extent it eliminates the threat of wrongful disclosure or use of the information (the only

---

59. FED. R. CIV. P. 65; *see* Daniels Health Scis., LLC v. Vascular Health Scis., LLC, 710 F.3d 579, 586 (5th Cir. 2013) (upholding a preliminary injunction granted in a case for misappropriation of trade secrets).

60. *See* 18 U.S.C. § 1519 (2012) (describing the penalty for destruction, alteration, or falsification of records in federal investigations and bankruptcy).

61. *See* FED. R. CIV. P. 16(b) committee note (2006) (regarding electronically stored information).

claim that is available if the information was voluntarily provided by the trade secret owner).

Admittedly, spoliation of evidence concerns pale in comparison to the potential use and disclosure of trade secrets themselves; thus, the latter concern provides a stronger argument in favor of the proposed seizure order. However, the magnitude of the problem seems overstated in light of practical solutions that already exist and the existing power of courts to render temporary restraining orders. For instance, sometimes in trade secret cases the alleged misappropriator has no interest in disclosing the alleged trade secrets because it is in his own competitive interest to keep such information secret, and thus there is little need for a quick seizure order. Similarly, trade secret misappropriation cases have settled when the defendant agrees to box up and seal whatever information (if any) he took from a former employer in order to prevent the information from being used or disclosed.

If, as appears to be the case, the proposed seizure order is designed to address the special case of espionage (cyber or otherwise), or more broadly the "improper means" prong of misappropriation, there is undoubtedly the threat of destruction of evidence because a foreign agent is likely to try to hide his tracks. However, as discussed in Part II.C, this is precisely the type of case that the EEA was designed to combat and that is likely to garner the attention of federal prosecutors, who have the power to obtain a search warrant. To the extent the concern is about federal prosecutors not acting frequently or quickly enough, that may be because there is little merit to the claims or because the case does not involve espionage but, rather, a dispute between competitors (which, as noted above, are the vast majority of trade secret cases). In an era of tight resources, trade secret claimants may take a back seat, particularly where the alleged trade secret(s) at issue may be nonexistent. It may also be because the EEA was adopted with the understanding that it would be used judiciously.[62]

---

62. *See* 28 C.F.R. § 0.64-5 (2014) (requiring U.S. attorneys to obtain the "personal approval of the Attorney General, the Deputy Attorney General, the Assistant Attorney General for National Security, or the Assistant Attorney General, Criminal Division" before filing charges under the EEA); U.S.

Critically, the seizure remedy gives powers to putative trade secret trolls far beyond those possessed by current patent trolls. The seizure remedy raises the same concerns that killed copyright's Stop Online Piracy Act (SOPA)[63] and Protect Intellectual Property Act (PIPA)[64] in 2011.[65] Like SOPA and PIPA's doomed provisions, the proposed civil seizure process is much broader than the impoundment remedy that exists under U.S. copyright and trademark law because it is not limited to allegedly infringing products. Instead, seizure would extend to wide swaths of information that need not include actual trade secrets. This powerful option makes the entire process even more suspect than existing copyright and trademark remedies and raises the specter of SOPA-like infirmities.

The chilling effect on innovation and job growth of receiving a threat of litigation under the Acts could be profound. Under the Acts' seizure remedy, mobile employees and fledgling start-up businesses might have the tools of their trade, including smartphones and computers, taken away from them based on an unproven accusation.[66] Even if the Acts include heightened requirements in order to obtain a seizure order, the courts may never get the chance to adjudicate the issue. Rather, the adjudication may happen in the marketplace, where the recipient of a trade secret troll's letter (which would threaten a seizure action) will have to decide if it has the capacity and resources to challenge the claim in court. If it does not—which would be the case for many potential recipients of such letters, from start-ups to struggling companies—the practical impact could be a settlement payment and, potentially, the end of the business. Innovation may be lost, jobs may be terminated, and lives may be

---

ATTORNEY MANUAL § 9-59.100 (2014), *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/59mcrm.htm (noting that the "EEA is not intended to criminalize every theft of trade secrets for which civil remedies may exist under state law").

63. H.R. 3261, 112th Cong. (2011).

64. S. 968, 112th Cong. (2011).

65. *See Professors' Letter*, *supra* note 14, at 6 n.10 (discussing the demise of SOPA and PIPA).

66. *See* Seaman, *supra* note 17, at 27–31 (describing the seizure remedy in the Acts).

devastated based upon an unproven allegation or a seizure remedy improperly issued. That eventuality is SOPA magnified, and is a major cause for alarm.

Moreover, the grant of this seizure remedy has no extraterritorial impact and, in any event, foreign courts are unlikely to enforce a U.S. court order issued *ex parte* without notice or an opportunity to be heard. Therefore, the seizure remedy may actually be a godsend to those who wish to diminish U.S. competitiveness; they would simultaneously empower trade secret trolls with vast ability to quash U.S. competition, while arming them with orders that have no meaningful impact outside the United States, where the alleged trade secrets are purportedly going! On this basis alone, the Acts should be reconsidered.

As if the above reasons were not enough to abandon the Acts, the proposed seizure remedy raises a number of constitutional concerns. First, any seizure or other preliminary order that requires an individual to turn over alleged trade secrets might, if complied with, amount to compelled testimony with respect to which the individual can assert the Fifth Amendment privilege against self-incrimination.[67] Moreover, it appears that the claimed need for a seizure power is being used to introduce the concept of a "civil search order" (also known as an Anton Piller Order[68]) into U.S. law. This concept is untested and of questionable constitutionality in the United States due to the search and seizure provisions of the Fourth Amendment to the U.S. Constitution.[69]

In sum, even if issues concerning the scope and meaning of the proposed seizure remedy could be resolved, there are few cases when it is actually needed. Many companies already have evidence preservation policies in place, and when there is concern that none exist, state and federal courts have the power to grant preliminary relief and other orders to preserve evidence. In

---

67. *See, e.g.*, Heddon v. State, 786 So. 2d 1262, 1263–64 (Fla. Dist. Ct. App. 2001) (holding that employee's Fifth Amendment privilege would prohibit forcing him to produce information in his possession).

68. Anton Piller K.G. v. Mfg. Processes, Ltd., [1975] EWCA (Civ) 12, [1976] Ch. 55 (Eng.).

69. U.S. CONST. amend. IV.

egregious cases of alleged espionage, there is an even better search and seizure remedy available for use by criminal prosecutors.

Even more troubling are the powers that the seizure authority would hand to the newly vivified trade secret trolls. Under the Acts, trade secret trolls would gain a powerful tool that could be used to significantly disrupt the business operation of a competitor. Although it is argued that it would only be rarely sought or granted, trolls, by definition, are predisposed not to worry that much about the merits of their claims because the greater the potential cost of litigation to their victims, the greater the potential for a quick settlement. Trade secret trolls operate based upon unsubstantiated threats of litigation, rather than a concern about losing in court. The Acts create conditions where trolling could become a highly lucrative business model, in which the sources of revenue are start-ups, innovators, workers, and society.

Thus, while ostensibly designed to address the problem of foreign espionage, given the fact that most trade secret cases involve domestic parties, the seizure remedy is more likely to be used to disrupt U.S. businesses. The free-ranging power of trade secret trolls to disrupt and destroy competitors through aggressive use of the Acts is reason enough to pass on these well-meaning but poorly conceived bills.

E. Federal Courts: "State Courts Will Not Handle These Cases in a Timely Fashion, So We Need the Acts."

This somewhat baffling assertion ties to the general belief that federal courts are much better equipped to handle cyberespionage than their state counterparts.[70] However, there is no comprehensive research or empirical data to back up the claim that state courts are ill equipped to handle trade secret cases. Instead, it seems to be based upon anecdotal experiences by certain plaintiffs in one or more states. Without examining the

---

70. *See* Almeling, *supra* note 40, at 794 n.109 (discussing whether state courts are able to address growing trade secret litigation); Seaman, *supra* note 17, at 51–52 (discussing the new availability of a federal forum under the Acts).

actual record of cases when an alleged lack of response occurred, it cannot be determined whether a court's refusal to hear or grant a motion for a temporary restraining order was actually based upon a lack of merit. The fact that many attorneys prefer to litigate in federal court should not be a reason for adopting a new federal cause of action.

The reality is that most trade secret misappropriation claims are brought in the larger industrialized and high-tech states that have special commercial courts or business law judges to handle trade secret claims. To suggest that the judges of these courts, who are likely to see numerous trade secret cases during their tenure, are not competent to handle trade secret cases is unjustified. Moreover, it is an affront to the U.S. system of government to suggest that the incompetence of state judges is a legitimate reason to adopt a federal law. We have many bodies of law, including commercial law, that we rightly allow states to develop and apply even though the resulting litigation may involve parties from multiple states and countries. The Uniform Commercial Code is but one example.

Far from being incapable of handling trade secret cases, state court judges are more apt to understand the social values and norms of their local community on such important issues as the meaning of "improper means" of acquiring trade secrets, the value of employee mobility, and the importance of free competition. They are also in a better position based upon the practices of local businesses and the availability of resources to understand what "reasonable efforts" are available locally to protect trade secrets. Lastly, unlike federal courts that often have to predict how a state court might rule on an issue, state court judges can actually make the rulings based upon their knowledge of state law. Thus, it is fair to say that state court judges will be and are as equipped to handle these complex matters and to identify the trolling behavior about which the authors are concerned.[71]

---

71. *See, e.g.*, Seaman, *supra* note 17, at 55–56 (discussing the drawbacks of litigating in a federal forum); *cf.* Almeling, *supra* note 26, at 293, 301 (discussing the frequency with which trade secret litigation is brought in federal court).

III. Alternatives

The risk of trade secret trolls, built around a primary concern about cyberespionage, has been largely absent in the history of trade secret law. They should be avoided, but Congress need not ignore the cyberespionage problem in order to abandon the Acts. Because there is no debate that trade secrets are important to U.S. businesses and that they are being misappropriated to some degree by foreign entities and agents, Congress should not simply throw its figurative hands up and walk away from the problem. Rather, Congress should consider ways to combat cyberespionage without damaging trade secret law and unintentionally summoning trade secret trolls.

This Article proposes a reorientation of focus around the tort of misappropriation rather than the property concern of whether a trade secret exists.[72] The following alternatives implement that theoretical reorientation. By focusing on the bad acts of misappropriation and deterring theft, rather than the asserted property value of trade secrets, Congress can avert the trolls and better address the real problem of cyberespionage.

A. Amend the Computer Fraud and Abuse Act

With respect to the most egregious forms of trade secret misappropriation—cyberespionage and foreign espionage—there are already two federal laws on the books to punish such behavior: the aforementioned EEA and the Computer Fraud and Abuse Act[73] (CFAA). The well-intentioned CFAA, designed to criminalize unauthorized intrusions into computer networks, is already notorious as an overbroad and ambiguous dragnet that implicates at least as much legal activity as it does illegal. Thus, it is in dire need of amendment to reflect what has been learned and experienced since it was enacted in the pre-Internet age.[74]

---

72. This concept is the focus of a work in progress by David S. Levine and Franck Pasquale currently titled *Tailoring Trade Secrecy: The Moral Imperative of Industry-Specific Application of Doctrine*.

73. 18 U.S.C. § 1030 (2012).

74. See Thomas Fox-Brewster, *Aaron's Law Is Doomed Leaving US Hacking Law 'Broken'*, FORBES (Aug. 6, 2014, 9:39 AM),

To more directly combat cyberespionage and enforce commercial ethics, the CFAA should be tailored to address current threats and existing bad acts rather than trade secrets specifically. In particular, the extraterritorial reach of the CFAA and the predicate wrongful acts should be reconsidered. Perceived problems with the existing language of the CFAA, which has exposed individuals to criminal prosecution for lesser acts of information access,[75] can be addressed at the same time. Fixing the CFAA can provide a bonus for trade secret plaintiffs if it is amended to allow security researchers greater ability to understand and analyze modern hacking and cybersecurity tactics without fear of running afoul of the law.[76] That research can be rolled into improving existing corporate cybersecurity abilities and standards.

There is also a political bonus in this proposed solution. Because of widespread criticism of the CFAA, there might be broad and bipartisan support for its reform. As there is little debate that the acquisition of private commercial information (be they trade secrets, proprietary information or otherwise) via wrongful computer access should be deterred, we recommend amending the CFAA to directly prohibit such behavior instead of passing the Acts.

B. Improve Cybersecurity Standards and Capabilities

As explained in a soon-to-be-published article by Sharon Sandeen,[77] the increased use of the "Cloud" to store and transfer

---

http://www.forbes.com/sites/thomasbrewster/2014/08/06/aarons-law-is-doomed-leaving-us-hacking-law-broken/ (last visited Jan. 11, 2015) ("There is a general agreement . . . that the CFAA needs an urgent update.") (on file with the Washington and Lee Law Review).

75. *See* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1135 (9th Cir. 2009) (finding that an employee who emailed himself work documents during extensive work travel did not violate the CFAA).

76. ELEC. FRONTIER FOUND., THE COMPUTER FRAUD AND ABUSE ACT HAMPERS SECURITY RESEARCH 2 (2014) ("The CFAA should protect white-hat hackers and give them incentives to continue their important work."), https://www.eff.org/files/filenode/cfaa-security-researchers.pdf.

77. Sharon Sandeen, *Lost in the Cloud: Information Flows and the Implications of Cloud Computing for Trade Secret Protection*, 19 VA. J.L. & TECH. (forthcoming 2015),

data undermines the trade secret status of stored information both from practical and legal standpoints. Congress might ameliorate such risks by enacting legislation to clarify that the mere storage of information in the Cloud (provided that other reasonable efforts are engaged in by the trade secret owner) is not a trade secrecy-waiving event. It should be noted that it is currently impossible to completely protect a commercial computer network from the most sophisticated and determined attackers, although intrusions, once detected, can be contained.[78] Nonetheless, the benefits of such a law might be conditioned on trade secret owners utilizing enhanced security tools, thereby providing an incentive for U.S. businesses to institute increased security measures.[79]

C. International Harmonization of Trade Secret Law and Principles

The existing international trade secret harmonization efforts are generally a good idea and should be continued,[80] but even if the laws of numerous countries are amended to conform more closely to U.S. norms, there is still a lack of understanding among businesses in the United States and elsewhere about what is necessary to create and protect trade secret information.[81] In this regard, self-help designed to prevent trade secret theft in the first instance is likely to be more effective and efficient than any new law, and without the negative consequences of trade secret trolls. The U.S. government should ramp up education in this area, perhaps by publishing Trade Secret Management Guidelines

---

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2490671.

78. *See* Villasenor, *supra* note 19 (discussing other means to protect trade secrets from cybersecurity intrusions).

79. *Id*.

80. Although the authors believe that they should be conducted in a more open manner. *See* Sean Flynn, *Sean Flynn, David Levine, Margot Kaminski: Comment to USTR on the Public Interest Trade Advisory Committee Proposal*, INFOJUSTICE.ORG (Mar, 25, 2014), http://infojustice.org/archives/32535 (last visited Jan. 11, 2015) (on file with the Washington and Lee Law Review).

81. *See* Villasenor, *supra* note 19 (discussing other means to protect trade secrets from cybersecurity intrusions).

similar to those published by the Japanese government.[82] We also recommend training of state court judges to address concerns about their inability to quickly address trade secret misappropriation claims.

D. Streamlined Cross-Border Discovery and Enforcement

Because much of the concern surrounding the proposed trade secret legislation is about the asserted difficulty of conducting discovery and enforcing judgments across borders, Congress should examine whether it can improve and streamline those procedures. This would not only be of value in trade secret cases, but in other commercial disputes as well. Indeed, the benefits of the uniform law process in the United States should not be ignored, suggesting that many problems that Congress perceives might be more effectively resolved through the use of such processes.

IV. Conclusion

The debate around the Acts is decidedly not about the existence of harms. Even though trade secrecy suffers the same dearth of data that has made the reaction to rampant copyright infringement a guessing game between copyright maximalists and civil society,[83] there is no question that U.S. companies face a

---

82. *See Release of Revised "Trade Secret Management Guidelines*," MINISTRY ECON., TRADE, & INDUSTRY (Dec. 1, 2011), http://www.meti.go.jp/english/press/2011/1201_01.html (last visited Jan. 16, 2015) (describing the contents of the Trade Secret Management Guidelines, which are not readily available in English) (on file with the Washington and Lee Law Review). The Federal Trade Commission offers guidance (albeit on the unrelated subject of advertising) in a similar format, which could serve as the model for propounding U.S. guidelines on the subject. *See Advertising and Marketing*, FED. TRADE COMMISSION, http://www.ftc.gov/tips-advice/business-center/advertising-and-marketing (last visited Jan. 16, 2015) (on file with the Washington and Lee Law Review).

83. This issue arose in the context of the battle over SOPA. *See* Yochai Benkler et al., *Social Mobilization and the Networked Public Sphere: Mapping the SOPA-PIPA Debate* (Berkman Ctr. Research Publ'n No. 2013-16, July 2013), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2295953.

mounting and complex threat from state-backed cyberespionage. The Sony scenario should only add to the perceived urgency. This Article is intended to orient the discussion about the Acts around the tort of misappropriation, which is the problem of cyberespionage, rather than the property right of trade secret ownership. The Article squarely addresses the arguments offered in favor of the Acts and explains the shortcomings of trade secret law as a solution, as well as the downside risks involving access to information and collaboration. Of equal importance, the Article proposes alternative avenues of exploration that have a much better chance of offering relief to beleaguered U.S. companies, their customers, and all who value commercial ethics in the marketplace of ideas.

We should all be alarmed by the possibility of creating conditions ripe for introducing trolling behavior into trade secrecy. Trade secret trolls have been unable to emerge thus far because of the strengths of uniform state law and the checks against abuse found in established trade secret principles and corollary state law involving noncompete covenants and invention ownership. But the free-ranging, plaintiff-oriented Acts will destroy that delicate balance and defeat the very purpose of trade secret law as a force of maintenance of commercial ethics. Simultaneously, the Acts will replace that balance by creating near-perfect conditions for the rise of trade secret trolls, moving cyberespionage from the first to the second most important issue in trade secrecy law and practice for trade secret holders.

For the foregoing reason in particular and, more generally, for all of the reasons discussed above, this Article urges abandonment of the Acts and offers other possible solutions. The Acts do much harm and little, if any, good. Let's leave trolls to the annals of science fiction (and patent law) and advance an environment where entrepreneurship, employee mobility, and legitimate access to information can flourish.