

THE MYTH OF THE TRADE SECRET TROLL:
WHY THE DEFEND TRADE SECRETS ACT IMPROVES
THE PROTECTION OF COMMERCIAL INFORMATION†

*James Pooley**

INTRODUCTION

Trade secret theft has been a federal crime since 1996, covered by the Economic Espionage Act of 1996¹ (“EEA”). But civil misappropriation claims remained limited to state court filings under common law or local variants of the Uniform Trade Secrets Act (“UTSA”). Calls for federal civil jurisdiction multiplied in the twenty years since the EEA’s passage, with the increasing importance of information as a business asset and with the emergence of technology that makes theft of these assets almost infinitely easier. Recent examples involving international actors galvanized the business community to request a straightforward solution: amend the EEA to provide a federal option for private claims.

Several bills were introduced in the 113th Congress to accomplish this and to authorize provisional remedies for seizure of relevant property to prevent secret technology from being transferred out of the jurisdiction. The 2014 legislation did not pass before Congress adjourned. A revised version, the Defend Trade Secrets Act (“DTSA”), was introduced in 2015—reflected in identical House (H.R. 3326)² and Senate (S. 1890)³ bills. After

† This is a revised version of an article that was originally published online as a draft in November 2015, discussing why the proposed Defend Trade Secrets Act deserved political support in spite of vigorous academic opposition. This version addresses the amended legislation as it was adopted, and refreshes arguments responding to that opposition.

* Mr. Pooley is a member of the California bar. He recently served as Deputy Director General of the World Intellectual Property Organization, an agency of the United Nations, where he was responsible for managing the international patent system. This service followed 37 years as a trial attorney handling hundreds of trade secret and patent disputes, many of them involving interstate and international actors. He has taught trade secret law and litigation as an adjunct professor at the University of California, Berkeley and at Santa Clara University. He is the author of the treatise “*Trade Secrets*,” first published by Law Journal Press in 1997 and continuously updated since then. His most recent business book is *Secrets: Managing Information Assets in the Age of Cyberespionage* (Verus Press 2015). An earlier version of this paper was presented at the 2015 Annual Conference of the George Mason University School of Law Center for the Protection of Intellectual Property. The author wishes to thank his fellow presenters and the audience for their useful feedback. He also wishes to thank Mark Schultz for helpful comments and Jaci Arthur for her research support.

¹ 18 U.S.C. §§ 1831-1839 (2012).

² H.R. 3326, 114th Cong. (2015).

hearings at which a number of amendments were made to the Senate bill, it passed with no opposition on April 4, 2016.⁴ The House accepted the amended Senate version, approving it on April 27, 2016, by a vote of 410 to 2.⁵ On May 11, 2016, President Obama signed the bill into law—now known as the Defend Trade Secrets Act of 2016.⁶

The legislation had received broad support from a variety of industries⁷ and also enjoyed unusually bipartisan political sponsorship.⁸ However, a group of thirty-one law professors submitted opposition to the predecessor bills in the form of an “open letter” dated August 26, 2014.⁹ Among other objections, they complained that the seizure provisions created inappropriate risks to third parties, that injunctions were not sufficiently limited, and that increasing the available remedies for misappropriation would lead to decreased employee mobility.¹⁰

Anticipating a renewed effort in the 114th Congress, several professors, including three of those who had signed the open letter, published journal articles that expanded on their concerns.¹¹ In the most recent of these, entitled *Here Come the Trade Secret Trolls*, a new argument was offered: that federalizing civil trade secret law would unleash a dangerous

³ S. 1890, 114th Cong. (2015).

⁴ *U.S. Senate Roll Call Votes 114th Congress—2nd Session*, SENATE.GOV, http://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=114&session=2&vote=00039 (last visited May 8, 2016) (indicating eighty-seven “Yeas” and thirteen “Not Voting”).

⁵ *Final Vote Results for Roll Call 172*, HOUSE.GOV, <http://clerk.house.gov/evs/2016/roll172.xml> (last visited May 8, 2016).

⁶ Pub. L. No. 114-153, 130 Stat. 376 (to be codified at 18 U.S.C. §§ 1832(b), 1833, 1835, 1836(b)-(d), 1839(3)-(7)).

⁷ See, e.g., Letter from Ass’n of Global Automakers, Inc. et al. to Senators Orrin Hatch, Christopher Coons & Jeff Flake (July 29, 2015), http://www.hatch.senate.gov/public/_cache/files/09ce963b-6166-4156-b924-ab1c7f4098f5/DTSA%20Senate%20Support%20Letter.pdf.

⁸ As of April 26, 2016, H.R. 3326 had 164 cosponsors, 104 Republicans and sixty Democrats, and S. 1890 had sixty-five cosponsors, thirty-six Republicans, twenty-eight Democrats, and one Independent. See *Cosponsors: S.1890—114th Cong. (2015-2016): Defend Trade Secrets Act of 2016*, CONGRESS.GOV, <https://www.congress.gov/bill/114th-congress/senate-bill/1890/cosponsors> (last visited May 6, 2016); *Cosponsors: H.R. 3326—114th Cong. (2015-2016): Defend Trade Secrets Act of 2015*, CONGRESS.GOV, <https://www.congress.gov/bill/114th-congress/house-bill/3326/cosponsors> (last visited May 6, 2016).

⁹ Letter from Professor Brook K. Baker et al. to the Sponsors of the Defend Trade Secrets Act of 2014 (S. 2267) and the Trade Secrets Protection Act of 2014 (H.R. 5233) (Aug. 26, 2014), <http://cyberlaw.stanford.edu/files/blogs/FINAL%20Professors%20Letter%20Opposing%20Trade%20Secret%20Legislation.pdf>.

¹⁰ *Id.*

¹¹ 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); David S. Levine & Sharon K. Sandeen, *Here Come the Trade Secret Trolls*, 71 WASH. & LEE L. REV. ONLINE 230 (2015); Christopher B. Seaman, *The Case Against Federalizing Trade Secrecy*, 101 VA. L. REV. 317 (2015).

new class of litigants called “trade secret trolls,” who—like their patent counterparts—would terrorize the community of legitimate innovators.¹²

On July 29, 2015, the DTSA was introduced simultaneously in the House and Senate.¹³ Among other modifications, the new version tightened the seizure requirements, limited certain injunctive relief, and constrained judicial orders that would block an employee from accepting a new job.¹⁴ On August 3, two authors of the *Trolls* article issued another open letter of their own, arguing that the changes were not enough and that the DTSA suffered from the same drawbacks as the previous proposals, leading to their prediction that it would “spawn a new intellectual property predator.”¹⁵ On November 17, those authors were joined by forty others in another open letter, contending that the legislation would harm small business, unduly restrict labor mobility, increase the cost of litigation, and disharmonize trade secret law.¹⁶

This Article offers a different perspective, informed not only by scholarship and public service, but also by a professional lifetime of experience handling trade secret litigation and trials. As explained in more detail below, federalizing civil trade secret law fills a critical gap in effective enforcement of private rights against cross-border misappropriation that has become too stealthy and quick to be dealt with predictably in state courts. The DTSA accomplishes this by effecting only very modest changes, relying heavily on existing laws and rules. The seizure provisions in particular are so narrowly drawn that only the most clearly aggrieved plaintiffs will risk invoking the procedure. Having no preemptive effect, the federal law leaves in place all relevant state laws and policies, allowing federal courts to address issues of concurrent jurisdiction as they have in other areas of the law. Finally, this Article argues that the specter of a new species of “trade secret troll” is so completely untethered to the realities of trade secret rights and disputes that it can safely be ignored.

¹² Levine & Sandeen, *supra* note 11, at 230.

¹³ Press Release, Doug Collins, Congressman, House of Representatives, “Defend Trade Secrets Act” Introduced in House and Senate (July 29, 2015), <http://dougcollins.house.gov/press-releases/defend-trade-secrets-act-introduced-in-house-and-senate/>.

¹⁴ H.R. 3326, 114th Cong. (2015).

¹⁵ David S. Levine & Sharon K. Sandeen, *Open Letter to the Sponsors of the Revised Defend Trade Secrets Act*, STANFORD CENTER INTERNET & SOC’Y, <http://cyberlaw.stanford.edu/publications/open-letter-sponsors-revised-defend-trade-secrets-act> (last visited May 6, 2016).

¹⁶ Letter from Professor Eric Goldman et al. to Senator Charles E. Grassley et al. in Opposition to the Defend Trade Secrets Act of 2015 (S. 1890, H.R. 3326) (Nov. 17, 2015), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2699760.

I. THE DEVELOPMENT OF U.S. TRADE SECRET LAW

Unlike other types of intellectual property that have always been defined by statute, the origins of trade secret protection lie in the common law, catalyzed by nineteenth-century industrialization that created a need to transfer and share secrets in business (which is why we refer to them as “trade” secrets).¹⁷ The law’s principles emerged from the results and reasoning of individual cases enforcing promises of confidentiality.¹⁸ Although many of the early cases emphasized the center of the inquiry as a confidential relationship that the law should respect, courts also recognized that the beneficiary enjoyed a property right in the expectation of secrecy.¹⁹ But courts’ logical emphasis on protecting a confidential relationship led the original framers of the *Restatement (First) of Torts* to categorize trade secrets within the law of torts.²⁰ Thus, Sections 757 through 759 of the First Restatement, published in 1939, represent the first step in “harmonizing” state common law of trade secrets.²¹ However, forty years later when the *Restatement (Second) of Torts* was published, trade secrets were not covered at all. The reporters explained that in the intervening years the fields of unfair competition and trade regulation had encroached to such an extent that tort law could no longer provide the central rationale, and it was left to a future restatement to address the issue.²²

This explanation was published about five years after the most important development in trade secret law of the twentieth century: the opinion of the United States Supreme Court in *Kewanee Oil Co. v. Bicron Corp.*,²³ in which petitioners claimed that state trade secret law should be preempted as conflicting with federal patent law, because the latter requires disclosure and the former protects against it.²⁴ Finding no preemption, the

¹⁷ See JAMES H. POOLEY, TRADE SECRETS § 1.02[8] (2014).

¹⁸ *Id.*

¹⁹ See *Peabody v. Norfolk*, 98 Mass. 452, 458 (1868) (“[One who] invents or discovers, and keeps secret, a process of manufacture . . . has a property in it, which a court of chancery will protect against one who in violation of contract and breach of confidence undertakes to apply it to his own use, or to disclose it to third persons.”). Whether or not trade secrets may be counted as “property”—some of the academic opponents of the DTSA think they should not—has long been debated, but because secret information can be transferred and taxed like other property, the question seems to be moot. See POOLEY, *supra* note 17, § 1.02[8].

²⁰ RESTATEMENT (FIRST) OF TORTS, §§ 757-759 (AM. LAW INST. 1939).

²¹ *Id.*

²² RESTATEMENT (SECOND) OF TORTS div. 9, introductory n. (AM. LAW INST. 1979) (“[T]he influence of Tort law has continued to decrease, so that it is now largely of historical interest and the law of Unfair Competition and Trade Regulation is no more dependent upon Tort law than it is on many other general fields of the law and upon broad statutory developments, particularly at the federal level.”).

²³ 416 U.S. 470 (1974).

²⁴ *Id.* at 472.

Court explained that trade secret law was grounded on important public interests: “[t]he maintenance of standards of commercial ethics and the encouragement of invention.”²⁵ Without guaranteed secrecy, businesses would be left to expensive self-help security measures that would disadvantage smaller competitors and discourage dissemination of information through sharing.²⁶ And, as a practical matter, there is no conflict between the two systems because they operate so differently: patent law is strong, providing an exclusive right “against the world,” while trade secret rights are “far weaker” because they do not protect against reverse engineering or independent development.²⁷

It was against this backdrop that the National Conference of Commissioners on Uniform State Laws in 1979 issued the first of two versions of the UTSA.²⁸ The need for the UTSA arose, according to the commissioners, because development of the law among the states had been “uneven,” and, therefore, the standards and remedies established by common law were uncertain.²⁹ Of course, the lack of treatment by the Second Restatement reinforced the need for an alternative path toward uniformity.

The UTSA tried to codify the fundamental principles of the existing common law of trade secrets, “preserving its essential distinction from patent law.”³⁰ But the common law had moved on since 1939, and the drafters of the UTSA effectively changed the Restatement rules in some significant ways. These shifts included broadening the scope of protection for information where its value was “actual or potential.”³¹ Section 757 of the First Restatement had required that secrets be “in continuous use” in a business.³² Now, “ephemeral” data (such as private bids) and “negative” secrets (such as the results of failed experiments) would be protectable.³³ On the other hand, under the First Restatement the trade secret owner’s self-help measures had been only a factor for consideration;³⁴ but under the UTSA

²⁵ *Id.* at 481. On the social interest in ethics, the Court also noted that there is an “inevitable cost to the basic decency of society when one firm steals from another.” *Id.* at 487.

²⁶ *Id.* at 485-86 (“The holder of a trade secret would not likely share his secret with a manufacturer who cannot be placed under binding legal obligation to pay a license fee or to protect the secret. The result would be to hoard rather than disseminate knowledge.”); *see also id.* at 493 (“Trade secret law promotes the sharing of knowledge, and the efficient operation of industry . . .”).

²⁷ *Id.* at 489-90 (“Where patent law acts as a barrier, trade secret law functions relatively as a sieve.”).

²⁸ UNIF. TRADE SECRETS ACT (NAT’L CONFERENCE OF COMM’RS ON UNIF. STATE LAWS 1985).

²⁹ *Id.* prefatory n.

³⁰ *Id.*

³¹ *Id.* § 1(4).

³² *Id.* § 1 cmt. 5.

³³ *Id.* § 1(4), § 1 cmt. 5.

³⁴ RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (AM. LAW. INST. 1939).

those “reasonable efforts” became part of the required proof to establish a protectable secret.³⁵

What could constitute a misappropriation was also changed. Under the First Restatement, mere acquisition of a secret, even if improper, was not actionable absent proof of use or further disclosure,³⁶ while the UTSA addressed acquisition where the actor had reason to know that it had been accomplished by improper means.³⁷ In the same vein, the First Restatement had provided “immunity” for third parties who received secret information in good faith,³⁸ whereas the UTSA adopted a rule that liability could be imposed following notice, subject to limited remedies based on a showing of innocent reliance by the user.³⁹

But, as its name suggests, a primary objective of the UTSA was uniformity.⁴⁰ On that score, the results have been disappointing. First, there are the two official versions, one issued in 1979 and the other in 1985 (mainly enhancing remedies), with a number of states having adopted the first before the second became available.⁴¹ And quite a few states have enacted a customized version of the official one.⁴² The notes to the UTSA acknowledge this by listing some of the individual states’ variations as annotations, adding a disclaimer that notes are not provided for states that “depart from the official text in such a manner that the various instances of substituted, omitted, and added matter cannot be clearly indicated by statutory notes.”⁴³ In other words, the variations are too numerous to mention.

³⁵ UNIF. TRADE SECRETS ACT § 1(4)(ii) (NAT’L CONFERENCE OF COMM’RS ON UNIF. STATE LAWS 1985).

³⁶ RESTATEMENT (FIRST) OF TORTS § 758 (AM. LAW. INST. 1939).

³⁷ UNIF. TRADE SECRETS ACT § 1(2)(i) (NAT’L CONFERENCE OF COMM’RS ON UNIF. STATE LAWS 1985); *see also* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 cmt. b (AM. LAW INST. 1995) (“The former Restatement of this topic imposed liability only for the wrongful use or disclosure of another’s trade secret. Improper acquisition of a trade secret was not independently actionable.”).

³⁸ RESTATEMENT (FIRST) OF TORTS § 758 cmt. b (AM. LAW INST. 1939).

³⁹ UNIF. TRADE SECRETS ACT § 2(b) (NAT’L CONFERENCE OF COMM’RS ON UNIF. STATE LAWS 1985).

⁴⁰ *Id.* prefatory n.

⁴¹ *See* Linda B. Samuels & Bryan K. Johnson, *The Uniform Trade Secrets Act: The States’ Response*, 24 CREIGHTON L. REV. 49, 51-53 (1990).

⁴² *See* Sid Leach, *Anything but Uniform: A State-By-State Comparison of the Key Differences in the Uniform Trade Secrets Act*, SNELL & WILMER (Oct. 23, 2015), <http://www.swlaw.com/assets/pdf/news/2015/10/23/How%20Uniform%20Is%20the%20Uniform%20Trade%20Secrets%20Act%20-%20by%20Sid%20Leach%20-%20AIPLA%20paper.pdf>.

⁴³ UNIF. TRADE SECRETS ACT general statutory n. (NAT’L CONFERENCE OF COMM’RS ON UNIF. STATE LAWS 1985). The annotations list sixteen state variations for Section 1 of the Act (definitions), seventeen for Section 2 (injunctive relief), seventeen for Section 3 (damages), seven for Section 4 (attorney’s fees), seven for Section 5 (preservation of secrecy), ten for Section 6 (limitations), and twenty-one for Section 7 (effect on other laws). *Id.* Only the title and the sections on severability and (ironically) uniformity have escaped modification by state legislatures.

Academics and practitioners have noted this lack of uniformity of the UTSA.⁴⁴ A few examples will help illustrate the scope of the problem. For one, California dropped the language requiring that a trade secret not be “readily ascertainable,” with the result that the defendant is required to specially plead that circumstance as an affirmative defense.⁴⁵ Illinois also eliminated the “readily ascertainable” language, and it prohibits royalty injunction orders, sets a different limitations period, and allows permanent injunctions.⁴⁶ Idaho requires that computer programs carry a “copyright or other proprietary or confidential marking” to qualify for protection.⁴⁷ Georgia limits protection of customer lists to physical embodiments, in effect allowing employees to appropriate such information in (human) memory.⁴⁸ And South Carolina’s version of the UTSA requires a court hearing an injunction request to consider “average rate of business growth” in determining a head start period and prescribes very particular rules for discovery of trade secret information, even for local discovery in aid of an action pending in another jurisdiction.⁴⁹

In 1995, the *Restatement (Third) of Unfair Competition* was released, including a new treatment of the law of trade secrets at Sections 39 through 45.⁵⁰ Although the new Restatement does an excellent job of summarizing and explaining the principles in a fashion broadly consistent with the UTSA, it has not yet achieved the level of acceptance that one might have hoped for. In fact, in states where the UTSA has not been adopted, courts still refer to the 1939 *Restatement (First) of Torts*, sometimes applying its (now minority) position on, for example, the need to show “continuous use” of secret information.⁵¹

In 1996, in recognition of substantial lacunae in existing federal criminal remedies, and with a particular focus on the challenge of foreign state-sponsored theft of trade secrets, the EEA was passed by Congress and

⁴⁴ See, e.g., David S. Almeling, *Four Reasons to Enact a Federal Trade Secrets Act*, 19 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 769, 773-74 (2009); Marina Lao, *Federalizing Trade Secrets Law in an Information Economy*, 59 OHIO ST. L.J. 1633, 1661-65 (1998); Christopher Rebel J. Pace, *The Case for a Federal Trade Secrets Act*, 8 HARV. J.L. & TECH. 427, 442-44 (1995).

⁴⁵ See James H. Pooley, *The Uniform Trade Secrets Act: California Civil Code § 3426*, 1 SANTA CLARA COMPUTER & HIGH TECH. L.J. 193, 197-98 (1985).

⁴⁶ 765 ILL. COMP. STAT. 1065/3 (2009).

⁴⁷ IDAHO CODE § 48-801(4)(c) (2015).

⁴⁸ See *Tronitec, Inc. v. Shealy*, 547 S.E.2d 749, 754 (Ga. Ct. App. 2001), *overruled on other grounds* by *Williams Gen. Corp. v. Stone*, 614 S.E.2d 758 (Ga. 2005).

⁴⁹ S.C. CODE ANN. §§ 39-8-50 to -60 (2016). For an accessible comparison of South Carolina’s current statute with its prior (and more conventional) version tracking the UTSA, see 2 BRIAN M. MALMBERG, *TRADE SECRETS: A STATE-BY-STATE SURVEY 2081* (4th ed. 2011).

⁵⁰ RESTATEMENT (THIRD) OF UNFAIR COMPETITION §§ 39-45 (AM. LAW. INST. 1995).

⁵¹ See, e.g., *Bear, Stearns Funding, Inc. v. Interface Group-Nevada, Inc.*, 361 F. Supp. 2d 283, 305-06 (S.D.N.Y. 2005) (applying “ephemeral events” exception); *Mann ex rel. Akst v. Cooper Tire Co.*, 816 N.Y.S.2d 45, 52-53 (N.Y. App. Div. 2006) (applying “continuous use” requirement to deny trade secret protection to formula for tire rubber).

signed into law.⁵² The process of legislative consideration was swift and bumpy, with some last-minute amendments.⁵³ In the years since its enactment, the EEA has had a mixed record of success. In the view of one veteran prosecutor, the average of about eight prosecutions per year is a “languid pace” that probably has done little to create a deterrent effect.⁵⁴ In part, this may be due to a reluctance of victims to bring cases to the prosecutor, either because of a loss of control or Fifth Amendment effects on civil claims,⁵⁵ or it may be due to a lack of resources or interest within the various offices of the U.S. Attorneys, who have discretion whether to accept qualifying cases.⁵⁶

II. PROPOSED LEGISLATION TO ADD A CIVIL CLAIM TO THE EEA

Calls for a federal trade secret law with a private right of action had already begun before the EEA was passed.⁵⁷ After it became law, scholars noted the anomaly and suggested that, because the national economy had become primarily knowledge-based, the UTSA failed to harmonize state trade secret law, and to bring the United States into full compliance with its obligations under the TRIPS Agreement,⁵⁸ a broad federal law should be enacted.⁵⁹ More recent commentary, while continuing to emphasize the drawbacks of variations in state law, also pointed out the economic advantages of federalization, particularly for small businesses, which rely more heavily on secrecy than on patenting,⁶⁰ as well as the procedural ad-

⁵² See generally James H.A. Pooley, Mark A. Lemley & Peter J. Toren, *Understanding the Economic Espionage Act of 1996*, 5 TEX. INTELL. PROP. L.J. 177 (1997).

⁵³ *Id.* at 187.

⁵⁴ Peter J. Toren, *An Analysis of Economic Espionage Act Prosecutions: What Companies Can Learn From It and What the Government Should Be Doing About It!*, 84 Pat. Trademark & Copyright J. (BNA) No. 2081, at 884 (Sept. 21, 2012), available at <http://petertoren.com/wp-content/uploads/2011/05/toren-eea2.pdf>.

⁵⁵ See Pooley, Lemley & Toren, *supra* note 52, at 219.

⁵⁶ *Id.* at 205; Toren, *supra* note 54.

⁵⁷ See, e.g., Pace, *supra* note 44, at 442-43 (arguing that variation in state laws applying to easily portable secrets made it difficult for larger companies to predict the outcome of disputes, and that the lack of a unifying federal statute raised questions about whether the United States was in full compliance with its obligations under international treaties).

⁵⁸ See Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), Including Trade in Counterfeit Goods, Dec. 15, 1993, 33 I.L.M. 81. Because the UTSA was used as the pattern for the international standard reflected in Article 39 of TRIPS, it is ironic that the United States has not established its own national standard but left civil enforcement exclusively in the hands of individual states.

⁵⁹ See, e.g., Lao, *supra* note 44, at 1674-79.

⁶⁰ See Almeling, *supra* note 44, at 782-88.

vantages for trade secret owners, including national service of process.⁶¹ Most commentators favoring a federal law have argued that it should explicitly preempt state law, in order to achieve the maximum benefits of uniformity. However, even a supplemental procedure—a choice of federal forum such as that provided by the DTSA—will likely provide most of the expected advantages, without having to overcome opponents’ arguments that states provide a useful “laboratory” for experimentation and that preemption might endanger important state policies.⁶²

Congressional efforts to provide a national civil claim for trade secret theft began in earnest in 2011, with the introduction of a proposed amendment to other legislation.⁶³ The amendment would have added a private civil remedy to the EEA, together with an *ex parte* seizure provision patterned on language from the Lanham Act.⁶⁴ That effort failed to secure a vote on the amendment.⁶⁵ The following year Senator Coons, along with Senators Kohl and Whitehouse, introduced S. 3389, the Protecting American Trade Secrets and Innovation Act, a revised and somewhat more comprehensive version of the 2011 proposal, using language from the EEA and UTSA to define the subject and remedies, and again including a provision for *ex parte* seizures on very specific showings.⁶⁶ The bill did not progress.

In the 113th Congress, several bills sought to create a private right of action under the EEA. The Defend Trade Secrets Act (S. 2267) (2014 DTSA), introduced by Senators Coons and Hatch, was substantially similar to S. 3389 from the previous Congress, although it proposed a limitations period of five years rather than three.⁶⁷ Earlier, Senator Flake introduced S. 1770 as the Future of American Innovation and Research Act, with language and provisions similar to the Coons-Hatch proposal, but maintaining a three-year limitations period and adding a section covering antisuit injunctions.⁶⁸ In the House, Congressman George Holding led a bipartisan group in submitting H.R. 5233, the Trade Secrets Protection Act of 2014 (“TSPA”), again with a structure similar to S. 2267 but providing more

⁶¹ R. Mark Halligan, *Protection of U.S. Trade Secret Assets: Critical Amendments to the Economic Espionage Act of 1996*, 7 J. MARSHALL REV. INTELL. PROP. L. 656, 667-68 (2008). Mr. Halligan updated his comprehensive treatment of the subject in R. Mark Halligan, *Revisited 2015: Protection of U.S. Trade Secret Assets: Critical Amendments to the Economic Espionage Act of 1996*, 14 J. MARSHALL REV. INTELL. PROP. L. 476 (2015).

⁶² See Seaman, *supra* note 11, at 365-67. The fear of federal trade secret law displacing any state’s rules on the separate question of noncompete covenants is overdone, even under a preemptive regime. However, the DTSA is explicitly nonpreemptive and, thus, the concern is even more abstract.

⁶³ 157 CONG. REC. 14,770-71 (2011).

⁶⁴ *Id.*

⁶⁵ *Id.*

⁶⁶ Protecting American Trade Secrets and Innovation Act of 2012, S. 3389, 112th Cong. (2012).

⁶⁷ Defend Trade Secrets Act of 2014, S. 2267, 113th Cong. (2014).

⁶⁸ Future of American Innovation and Research Act of 2013, S. 1770, 113th Cong. (2013).

detailed constraints on the seizure process.⁶⁹ Finally, Congresswoman Zoe Lofgren introduced H.R. 2466, the Private Right of Action Against Theft of Trade Secrets Act, a two-paragraph amendment to the EEA that would have added a civil cause of action, but without the *ex parte* seizure provisions.⁷⁰ The TSPA was favorably reported out of committee, but no other action was taken, and all four bills expired at the end of the 113th Congress.⁷¹

III. LAW PROFESSORS' OPPOSITION

While industry expressed virtually unanimous support for the 2014 DTSA and the TSPA, and both received unusually bipartisan backing, opposition to the bills arrived in the form of a letter signed by thirty-one law professors engaged in “intellectual property law, trade secret law, innovation policy and/or information law.”⁷² The letter argued that there was no apparent need for the legislation because “effective and uniform state law already exists,” current procedures for interstate and foreign process were adequate, and access to federal courts for state law claims was available under diversity jurisdiction.⁷³ It claimed that the bills would not solve any perceived problems because they would leave in place potentially determinative “ancillary state law” issues and because they failed to address the challenge of establishing jurisdiction over foreign actors.⁷⁴ And it complained that enactment of the legislation would cause serious harm by imposing a dangerous process for *ex parte* seizures, ignoring the right to reverse engineer, and raising the prospect of indefinite injunctions.⁷⁵ Requiring definition of secrets early in litigation to address jurisdiction issues, it added, could increase the risk of improper disclosure.⁷⁶ Finally, it suggested that the new laws could be used “as an additional weapon to prevent public and regulatory access to information, collaboration amongst businesses, and mobility of labor.”⁷⁷ Congress, the letter concluded, should redirect its attention away from trade secret misappropriation and instead focus on legislation to combat “cyber-espionage and foreign espionage.”⁷⁸

⁶⁹ Trade Secrets Protection Act of 2014, H.R. 5233, 113th Cong (2014).

⁷⁰ Private Right of Action Against Theft of Trade Secrets Act of 2013, H.R. 2466, 113th Cong (2013).

⁷¹ See *H.R. 5233—Trade Secrets Protection Act of 2014*, CONGRESS.GOV, <https://www.congress.gov/bill/113th-congress/house-bill/5233/actions> (last visited May 6, 2016).

⁷² Baker et al., *supra* note 9, at 1.

⁷³ *Id.* at 2-3.

⁷⁴ *Id.* at 3.

⁷⁵ *Id.* at 4-5.

⁷⁶ *Id.* at 5.

⁷⁷ *Id.*

⁷⁸ Baker et al., *supra* note 9, at 7.

The professors' letter was followed months later by several published articles that correctly anticipated continuing efforts in the 114th Congress to federalize trade secret law.⁷⁹ This Article provides a brief summary and critique of those articles below, as a prelude to a more thorough discussion of the DTSA as it was amended and enacted, but at this point it responds briefly to the arguments raised in the 2014 letter and then to those raised in the letter of November 17, 2015.

While reasonable people can disagree over how much variation among state statutes can be accepted while still calling them "uniform," it should be apparent from the examples provided in the background section of this Article that the UTSA cannot fairly be deemed "uniform" without serious caveats. But in the 2014 letter, there was no acknowledgement of the substantial variation that exists and that can bedevil companies with operations in multiple states. Cross-border procedural hurdles are not made to disappear by the "rich body of law" that informs how to deal with them.⁸⁰ And diversity jurisdiction must rest on complete diversity of citizenship,⁸¹ which does not exist in the common trade secret case that involves one or more local actors.

Although a nonpreemptive federal statute could lead to related issues of state law being resolved in some cases, federal courts have demonstrated in other areas of concurrent jurisdiction that they are quite capable of resolving those issues.⁸² They have also proven capable of using protective orders to prevent loss of secrecy in the courtroom.⁸³ In addition, it is safe to assume that, because of their generally more extensive experience with international litigation, federal judges are well equipped to efficiently handle difficult questions of personal jurisdiction over foreign defendants. The professors' initial concerns over the *ex parte* seizure provisions, protecting the right to reverse engineer, and appropriate limitations on injunctions were legitimate. But, as should become clear in the discussion that follows, those concerns have been adequately addressed by the legislation as it was enacted.

The professors' last cluster of arguments in their 2014 letter is the most troubling.⁸⁴ Simply put, the idea that collaboration among businesses would somehow be diminished because litigants could sue in federal court makes no sense. Indeed, it is the very existence of judicial remedies for misappropriation that makes business collaboration possible.⁸⁵ As the Su-

⁷⁹ See *infra* notes 101-127 and accompanying text.

⁸⁰ Baker et al., *supra* note 9, at 3.

⁸¹ *Lincoln Prop. Co. v. Roche*, 546 U.S. 81, 89 (2005).

⁸² 20 AM. JUR. 2D *Courts* § 88, Westlaw (database updated Feb. 2016).

⁸³ As a response to this, there have been movements to restrict protective orders. See, e.g., Arthur R. Miller, *Confidentiality, Protective Orders, and Public Access to the Courts*, 105 HARV. L. REV. 427, 441-42 (1991).

⁸⁴ See Baker et al., *supra* note 9, at 5-6.

⁸⁵ See *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 486 (1974).

preme Court explained in *Kewanee Oil*: “The holder of a trade secret would not likely share his secret with a manufacturer who cannot be placed under binding legal obligation to pay a license fee or to protect the secret. The result [of preempting trade secret law] would be to hoard rather than disseminate knowledge.”⁸⁶

Similarly, the proposition that adding a federal civil cause of action for misappropriation would reduce public or regulatory access to critical information is a non sequitur. The DTSA affects only a private interest in information, and the Freedom of Information Act and other statutes that form the federal edifice of health and safety regulation have not been changed. Finally, the professors’ concern over mobility of labor was misplaced for similar reasons. If their worry was about enforcement of non-competition covenants, the answer is that the DTSA, having no preemptive effect, will not impact state law or policy in that area. And, as will be discussed, anxiety over application of the “inevitable disclosure doctrine” was overdone and in any event should now be completely resolved.⁸⁷

The 2015 professors’ letter made several new or revised arguments, all of which were hypothetical and weak. First, while admitting that the originally proposed language on ex parte seizure was “more limited in scope” than the 2014 legislation (for example, only property “necessary to prevent the propagation or dissemination of the trade secret” could be seized), the professors complained that this tightening was not enough and that the provision “may still result in significant harm.”⁸⁸ The letter provided no evidence for this,⁸⁹ but speculated that mere invocation of the procedure might cause “start-up companies” to “capitulate” and that the “chilling effect on innovation and job growth . . . could be profound.”⁹⁰ As will be explained below, these abstract fears were, and are, ungrounded and exaggerated.⁹¹

Second, the letter asserted that new language, added to ensure that mobility of labor is respected, embraced the so-called “inevitable disclosure

⁸⁶ *Id.*

⁸⁷ *See infra* Part VII.

⁸⁸ Goldman et al., *supra* note 16, at 3 & n.5.

⁸⁹ The letter relied in part on a brief essay which itself appears to have drawn from the professors’ earlier correspondence. John Tanski, *The Defend Trade Secrets Act Is Strong Medicine. Is It Too Strong?*, CORPORATE COUNSEL (Oct. 30, 2015), <http://www.corpcounsel.com/id=1202741205249/The-Defend-Trade-Secrets-Act-Is-Strong-Medicine-Is-It-Too-Strong?slreturn=20151009142017>. The author incorrectly asserted that the DTSA would allow a court to “shut down the defendant’s business for up to a week.” *Id.* His fears of “trade secret trolling” were based on the claim that trade secret law covers so much information that “it is easy for unscrupulous plaintiffs to manufacture trade secret claims and use them as strategic weapons.” *Id.* But he failed to acknowledge that this broad scope of the law has not led to any epidemic of false claims in state courts, much less explain why nuisance suits or the imagined “trolls” would be more likely to emerge under the scrutiny of federal judges.

⁹⁰ Goldman et al., *supra* note 16, at 4 (quoting Levine & Sandeen, *supra* note 11, at 255) (internal quotation marks omitted).

⁹¹ *See infra* Part VII.

doctrine,” which is nothing more than a method of analysis under the UTSA provision for injunctions against “threatened misappropriation.”⁹² Although this often-misunderstood method has been applied in a majority of jurisdictions, where the evidence has led to a wide range of remedies falling far short of prohibiting competitive employment, the professors’ position is based on the false premise that the doctrine amounts to a judge-made noncompetition agreement.⁹³ This Article explains below in more detail why this is a straw man argument.⁹⁴

Third, the professors claimed that the DTSA “likely will increase the length and cost of trade secret litigation,” with consequential damage to “small businesses and startups.”⁹⁵ As with many of their other points of opposition, this one lacked any empirical support. Although the DTSA only applies to trade secrets that are “related to a product or service used in, or intended for use in, interstate or foreign commerce,” there is nothing in our experience with similar federal laws that would suggest this requirement could not easily and quickly be met with uncontroverted proof, much less that it would “both delay the case and result in increased costs” of litigation.⁹⁶ And although the letter cited survey evidence demonstrating the substantial cost of trade secret litigation, that applies equally in state court proceedings where discovery can be as extensive and produce as many collateral disputes.⁹⁷

Finally, the letter returned to the argument made in 2014, that existing state law is “coherent,” “robust and uniform,” so that U.S. businesses already enjoy “a high level of predictability.”⁹⁸ As has already been pointed out, this dismissive rhetoric hardly obscures the reality of a patchwork of differing standards and rules—in some ways more divergent than before enactment of the UTSA—that necessarily create friction and inefficiency for companies with interstate operations. One might suppose that is why the DTSA has enjoyed such broad support in the business community. The

⁹² Goldman et al., *supra* note 16, at 4-5.

⁹³ The letter claimed—without citation of evidence or authority—that, in states that recognize the concept of inevitable disclosure, “the typical remedy is to enjoin the departing employee from commencing employment until the subject trade secret information is no longer a trade secret.” Goldman et al., *supra* note 16, at 4-5. However, a review of the case law reveals instead that “the outcome usually will not be an outright ban on employment, but a more limited injunction that permits the employee to go to work but forbids participation in some particular product line or area of the business.” POOLEY, *supra* note 17, § 7.02[2]. Orders not to take a job are “exceptional” and usually occur only when some form of noncompetition agreement is already in place, or there is clear evidence of fraud or bad faith. *Id.*

⁹⁴ See *infra* note 122 and accompanying text.

⁹⁵ Goldman et al., *supra* note 16, at 5.

⁹⁶ *Id.* at 6.

⁹⁷ *Id.* (citing AM. INTELLECTUAL PROP. LAW ASS’N, REPORT OF THE ECONOMIC SURVEY 2015, at 39, I-166, I-169 (2015)). Indeed, there is reason to believe that federal courts, applying the newly reinforced requirement of “proportionality” in the FRCP, will exercise their authority to rein in wasteful discovery practices. FED. R. CIV. P. 26.

⁹⁸ Goldman et al., *supra* note 16, at 7 (citing Baker et al., *supra* note 9, at 2).

professors also claimed, without offering analysis or examples, that whatever uniformity now exists will be undermined by the EEA's supposedly "broader" definition of a trade secret.⁹⁹ Finally, they pointed out the obvious: by failing to make the federal law preemptive, the trade secret holder will have a choice of forum, which they characterize as "forum shopping."¹⁰⁰

This Article now turns to the law review articles that followed issuance of the 2014 professors' letter. The first of these, by Professor Zoe Argento, is entitled *Killing the Golden Goose: The Dangers of Strengthening Domestic Trade Secret Rights in Response to Cyber-Misappropriation*.¹⁰¹ It treats the issue of cyber-espionage comprehensively and clearly, but that strength highlights the main problem with its logical structure. In her attack on the legislation, Professor Argento begins by assuming that the only problem to be solved is cyber-espionage.¹⁰² From there she proceeds to critique the proposed legislation mainly on the basis that it would not solve that problem.¹⁰³ And while it is undoubtedly true that giving private parties the right to sue in federal court is unlikely to put much of a dent in the international hacking scourge, that is certainly not the only problem that the DTSA was intended to confront. Instead, its main objective is to make it more practical for trade secret owners, now that their rights can be electronically compromised in mere seconds, to secure effective judicial relief.¹⁰⁴

While some of the other propositions advanced in the Argento article are problematic, in particular her treatment of the "property" theory,¹⁰⁵ it is

⁹⁹ *Id.* In fact, the EEA and the UTSA merely use different exemplary terms to express precisely the same idea: that the potential scope of trade secret protection is almost infinite. The EEA includes "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes." 18 U.S.C. § 1839(3) (2012). But every one of those categories also qualifies under the UTSA definition, which applies to "information, including a formula, pattern, compilation, program, device, method, technique, or process." UNIF. TRADE SECRETS ACT § 1(4) (NAT'L CONFERENCE OF COMM'RS ON UNIF. STATE LAWS 1985).

¹⁰⁰ Goldman et al., *supra* note 16, at 8.

¹⁰¹ See Argento, *supra* note 11.

¹⁰² See *id.* at 177.

¹⁰³ See *id.* at 214 (arguing that strengthening trade secret law would have little effect on cyber-misappropriation).

¹⁰⁴ See, e.g., Press Release, Office of Senator Christopher Coons, Senators Coons, Hatch Introduce Bill to Combat Theft of Trade Secrets and Protect Jobs (Apr. 29, 2014), https://www.legistorm.com/stormfeed/view_rss/527840/member/2812.html.

¹⁰⁵ See Argento, *supra* note 11, at 182-86 (equating the policy objective of encouraging innovation with a "property theory" (in contrast to a "tort theory" focusing on ethical behavior) that is supposedly inimical to the free movement of labor because it grants "exclusive rights" to the trade secret holder). However, the dispute between the "property" and "confidence" schools of thought is of historical interest only, and modern law recognizes both interests. See *supra* note 22 and accompanying text. In addition, Professor Argento's choice of vague and undefined terms in relation to trade secret law, such as "over-protection," "over-broad," and "strong" protection, is also too ambiguous to be useful. See Ar-

helpful to point out a few of her illuminating statements. First, she acknowledges that the North Carolina and Alabama trade secret statutes “vary significantly” from the UTSA.¹⁰⁶ She also agrees that significant advantages come with access to federal courts, noting that actors in a case involving cyber theft are “more likely to reside in a different state or even a different country” and that discovery is much more of a challenge in state court, where the proponent has to petition the courts of both relevant states.¹⁰⁷

The second major article to appear in opposition to the proposed legislation is by Professor Christopher Seaman, entitled *The Case Against Federalizing Trade Secrecy*.¹⁰⁸ This is a prodigious and scholarly work, comprising 77 pages and 492 footnotes. But it is worth the read. Professor Seaman leaves no reasonable issue untouched in his review of the law that provides context for the DTSA, and his analysis is generally fair and often insightful. However, in line with the professors’ letters, he overstates the extent of trade secret law harmonization that has been achieved by the UTSA and as a result minimizes the benefit of a unifying federal influence.¹⁰⁹ And while one of his key theses is that federalization risks abandoning the advantage of the states as “laboratories” for experimentation with differing policies,¹¹⁰ he gives little weight to the fact that the bills are expressly non-preemptive, leaving the states free to test policy choices as they wish.¹¹¹

Also in line with the first professors’ letter, Professor Seaman laments what he sees as an inverse relationship between the “strength” of trade secret law and the amount of useful information that is made available to the

gento, *supra* note 11, at 174-75. Experience shows that this kind of value-freighted terminology is frequently used in place of rigorous analysis of the competing interests that are almost always present in this area of the law.

¹⁰⁶ Argento, *supra* note 11, at 178 n.23 (“[S]ome states, particularly North Carolina and Alabama, have adopted versions of the statute which vary significantly from the UTSA.”); *id.* at 208 n.204 (“States vary on what constitutes misappropriation, the definition of a trade secret, the length of injunctions, exemplary damages, attorney fees, and the statute of limitations.”).

¹⁰⁷ *Id.* at 210.

¹⁰⁸ Seaman, *supra* note 8.

¹⁰⁹ For example, Professor Seaman says that “most jurisdictions follow the UTSA’s substance on the main points and depart only on less frequently encountered issues, such as the availability and amount of exemplary (punitive) damages.” *Id.* at 354 (footnote omitted). He is probably correct that “most” of the forty-seven jurisdictions follow the substance of the UTSA, but that leaves quite a few whose variations can matter quite a bit depending on circumstance. For example, the attorney appearing in a California case and unaware of its special requirement to plead ready ascertainability is likely to neglect that procedural detail and, as a result, waive the substantive claim. Similarly, when Professor Seaman points out that “only” eight states provide different limitations periods, he is making a value judgment that companies dealing with these differences may not share. *Id.* at 355.

¹¹⁰ *Id.* at 365.

¹¹¹ *Id.* at 360 (“Federal legislation that does not preempt state law ultimately will undermine harmonization, rather than promote it, by creating a federal regime that exists in parallel with state trade secret law.”).

public.¹¹² In fact, he hypothesizes a “bell curve” in which “weak” protection of secrets will (as *Kewanee Oil* recognized) lead to less disclosure, but in which “too much trade secret protection” will have the same result.¹¹³ There are multiple problems with this construct, not the least of which is the elusive abstraction of “strength” of the law and how to measure it. That failing shows up clearly when one tries to apply the notion to the DTSA. Just what is “too strong” in this context?¹¹⁴ The way he uses the phrase conflates the substantive (scope of rights) with the procedural (choice of court where rights will be enforced). If one considers the shift in trade secret law from the 1939 First Restatement to the modern rule of the UTSA, there has undoubtedly been some “strengthening.” But, by any rational comparison, the modest procedural changes inherent in the DTSA amount to more of a tweak than a departure.

Along the same lines, Professor Seaman argues that “federalizing trade secrecy would create more robust rights against extraterritorial conduct compared to patent law.”¹¹⁵ The observation seems intuitively correct, but why is that a problem? Patents are a strictly territorial, government-granted franchise, while trade secrets are established by a private relationship of confidence, the violation of which is commonly addressed wherever the parties are located, the bad behavior occurs, or its effects are felt.¹¹⁶

Like Professor Argento, Professor Seaman acknowledges that there could be benefits accruing to trade secret owners from having access to a federal forum. Specifically, he agrees that there is “some force” to the claimed advantages of nationwide service of process, broader jurisdictional reach over foreign defendants, more liberal discovery rules, and greater experience of federal judges in handling “complex IP and commercial disputes.”¹¹⁷ But he argues that litigants can achieve these benefits without

¹¹² *Id.* at 375 (“[T]he strengthening of trade secret protection via federalization likely will cause more inventors to opt out of the patent system in favor of trade secret protection, ultimately reducing the amount of available information about patentable inventions.”).

¹¹³ *Id.* at 385.

¹¹⁴ The “strength” abstraction runs out of control when Professor Seaman speculates that, if Congress passes the DTSA, later it “may enact additional changes that further strengthen the rights of trade secret owners.” Seaman, *supra* note 11, at 382.

¹¹⁵ *Id.* at 380.

¹¹⁶ See POOLEY, *supra* note 17, §10.07[4]. In *TianRui Group Co. v. International Trade Commission*, Judge Moore complained that extraterritorial application of U.S. trade secret law to a misappropriation occurring entirely in a foreign country would provide an “additional incentive to inventors to keep their innovation secret,” which would in turn “den[y] society the benefits of disclosure stemming from the patent system, which are anathema to trade secrets.” 661 F.3d 1322, 1343 (Fed. Cir. 2011) (Moore, J., dissenting). While robust domestic remedies for foreign theft of secrets belonging to U.S. companies can provide some additional encouragement to rely on secrecy, this is fully consistent with the Supreme Court’s holding in *Kewanee Oil* that trade secret law is complementary to the patent system. After all, the policy goal of patent law is not disclosure itself but encouragement of invention, and that is also a primary policy behind trade secret law. *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 493 (1974).

¹¹⁷ See Seaman, *supra* note 11, at 368.

amending the EEA by asserting their rights to federal diversity and supplemental jurisdiction.¹¹⁸ However, as already noted, complete diversity is often not present in trade secret disputes, and supplemental jurisdiction requires a common set of “central facts,” which also is frequently absent.¹¹⁹ Indeed, the weakness of his argument is underscored by his proposed alternative to the DTSA: Congress should remove the complete diversity requirement just for trade secret cases.¹²⁰

The most unusual of the three articles is *Here Come the Trade Secret Trolls*, by Professors David Levine and Sharon Sandeen.¹²¹ It relies heavily on the Argento¹²² and Seaman articles but does not supply any new evidence or fresh analysis.¹²³ Instead, its main contribution is to repeat in various ways a strikingly implausible prediction: that the DTSA would “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.”¹²⁴

“Patent troll” is a pejorative term deriving from the child’s story about a troll who surprised unsuspecting passers-by to demand payment for crossing a bridge. It is most often applied to companies whose only business consists of buying up and asserting patent rights. The metaphor works in that context because patents are an easily alienable right issued by the government, are effective “against the world,” and can be infringed regardless of fault.¹²⁵ Trade secrets, in stark contrast, are private rights that can be as-

¹¹⁸ *Id.* at 369.

¹¹⁹ See 28 U.S.C. § 1367 (2012); *United Mine Workers of Am. v. Gibbs*, 383 U.S. 715, 725 (1966); *Tech Enters., Inc. v. Wiest*, 428 F. Supp. 2d 896, 902 (W.D. Wis. 2006) (dismissing trade secret claim because it did not share a “common nucleus of operative facts” with a trademark claim).

¹²⁰ See Seaman, *supra* note 8, at 386-87.

¹²¹ See Levine & Sandeen, *supra* note 11.

¹²² Like Professor Argento, Professors Levine and Sandeen begin their attack on the legislation by assuming incorrectly that the only issue being addressed is cyberhacking. Levine & Sandeen, *supra* note 11, at 233. For this assumption they rely on a press release from Senator Coons’ office. *Id.* at 233-34. But even that selected document does not demonstrate such a narrow focus: “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.” Press Release, Office of Senator Christopher Coons, *supra* note 104. In other words, the core problem arises from changes in technology and the globalization of business. The authors’ straw man attack then becomes an argument that more data on cyberhacking is needed before considering legislation. See Levine & Sandeen, *supra* note 11, at 238.

¹²³ Indeed, many of its propositions are notable for the lack of any evidence or analysis. For example, the authors dismiss concerns over variations in state versions of the UTSA as “some minor but insignificant differences,” without addressing why the variations should not matter. *Id.* at 243. And they trivialize the advantages of a federal choice of forum by simply asserting, without citing any reference, that existing laws addressing interstate discovery “are not onerous” and that trade secret lawsuits involving foreign defendants are “rare.” *Id.* at 251.

¹²⁴ *Id.* at 252.

¹²⁵ Jacob S. Sherkow, *Patent Infringement as Criminal Conduct*, 19 MICH. TELECOMM. & TECH. L. REV. 1, 20-21 (2012).

served only against a thief or one who has breached a confidence.¹²⁶ Although frivolous trade secret lawsuits have occasionally been filed, existing law has sufficient sanctions to deal with those instances, and the DTSA contains precisely the same penalties.¹²⁷ As will be explained in more detail below, there never has been such a thing as a “trade secret troll,” and there is no reason to believe that the DTSA will cause this imagined beast to materialize.

IV. THE 2015 LEGISLATION, AS AMENDED AND ADOPTED IN 2016

The DTSA was introduced by identical bills filed in the Senate (S. 1890) and House (H.R. 3326) on July 29, 2015. For the most part, the legislation sought to amend 18 U.S.C. § 1836—created by the EEA in 1996—to provide a civil cause of action for any “person . . . aggrieved by a misappropriation of a trade secret” related to interstate commerce, adding sections on civil seizure and defining remedies for misappropriation.¹²⁸

At a Senate Judiciary Committee markup hearing on January 28, 2016, a “substitute” bill was presented, containing amendments that had been negotiated since an earlier hearing on December 2, 2015.¹²⁹ In general, these amendments were directed at harmonizing definitions with the UTSA, tightening further the seizure provisions, and dealing with the employee mobility issue by qualifying the scope of injunctions against “threatened” misappropriation. In addition, Senators Leahy and Grassley proposed a separate amendment establishing immunity from trade secret claims for employee whistleblowers who disclose information in confidence to law enforcement officials or in a sealed filing.¹³⁰ All amendments were accepted and the resulting bill passed the full Senate as well as the House without further amendment.

¹²⁶ Robert G. Bone, *The (Still) Shaky Foundations of Trade Secret Law*, 92 TEX. L. REV. 1803, 1805-06 (2014).

¹²⁷ *Compare* Defend Trade Secrets Act (DTSA) of 2016, Pub. L. No. 114-153, § 2(a), 130 Stat. 376, 380 (to be codified at 18 U.S.C. § 1836(b)(3)(D)), *with* UNIF. TRADE SECRETS ACT § 4 (NAT’L CONFERENCE OF COMM’RS ON UNIFORM STATE LAWS 1985).

¹²⁸ H.R. 3326, 114th Cong. § 2(a) (2015); *see also* S. 1890, 114th Cong. § 2(a) (2015) (using substantially similar language but without the term “aggrieved”). The DTSA adopted the Senate language. DTSA § 2(a), 130 Stat. at 376 (to be codified at 18 U.S.C. § 1836(b)(1)).

¹²⁹ S. 1890, 114th Cong. (as amended by substitute, Jan. 28, 2016), http://www.judiciary.senate.gov/download/s1890-substitute-amendment_-ehf16041. For the proceeding of the December 2 hearing, see *Protecting Trade Secrets: The Impact of Trade Secret Theft on American Competitiveness and Potential Solutions to Reedy This Harm*, U.S. SENATE COMM. ON JUDICIARY (Dec. 2, 2015), <http://www.judiciary.senate.gov/meetings/protecting-trade-secrets-the-impact-of-trade-secret-theft-on-american-competitiveness-and-potential-solutions-to-remedy-this-harm>.

¹³⁰ Amendment to S. 1890, 114th Cong. (as proposed by Sens. Leahy and Grassley, Jan. 28, 2016), http://www.judiciary.senate.gov/download/s1890-leahy-grassley1_-alb16037 (adding language that would become section 7 of the DTSA, to be codified at 18 U.S.C. § 1833).

The provisions covering ex parte seizure of property are extensive and tightly drawn. An application may only be granted in “extraordinary circumstances,” and it must be accompanied by a sworn affidavit from which it “clearly” appears “from specific facts” that injunctive orders under Rule 65 of the Federal Rules of Civil Procedure (“FRCP”) or other equitable relief would be insufficient because the defendant would evade them, that the seizure is necessary to prevent immediate and irreparable injury to the trade secret holder, and that the harm from refusing the order would exceed the harm to the defendant or any third party from issuing it.¹³¹ The application must also demonstrate likelihood of prevailing on the elements of the misappropriation claim, describe with particularity the material to be seized, demonstrate that the target of the seizure has actual possession of the material, prove the danger that it will be moved or lost, and certify that there has been no publicity of the requested seizure.¹³²

Seizure orders cannot be issued in summary form, but are required to contain findings of fact and conclusions of law, and must be drawn as narrowly as possible to achieve their purpose while minimizing interruption of any third party’s business as well as the defendant’s legitimate operations.¹³³ They must also provide guidance to law enforcement about the timing of the seizure and any authorized use of force. The plaintiff may not participate in the seizure, which must be made by federal officials assisted only by an independent technical expert, nor can the plaintiff be given access to any of the seized material. The material must be taken into the court’s custody, available only to an appointed special master tasked with separating and “facilitat[ing] the return of unrelated property and data.”¹³⁴ The plaintiff must post a bond to secure liability in case the seizure turns out not to have been justified, but the amount of the bond will not limit damages that can be claimed for wrongful seizure.¹³⁵ The order may remain in effect only seven days before a hearing is held, at which the plaintiff must show facts justifying continuation of the order and the court may modify the normal discovery timeframes.¹³⁶

Following execution of the seizure order, the defendant or anyone else affected can move at any time to dissolve or modify it.¹³⁷ The court must hold the seized property, and electronic files will be kept unconnected with any network, including the Internet.¹³⁸ Access must be controlled, and no

¹³¹ 18 U.S.C.A. § 1836(b)(2)(A)(i)-(ii) (West 2016).

¹³² *Id.* § 1836(b)(2)(A)(ii)(IV)-(VIII).

¹³³ *Id.* § 1836(b)(2)(B)(i)-(ii).

¹³⁴ *Id.* § 1836(b)(2)(D)(iv).

¹³⁵ *Id.* § 1836(b)(2)(B)(vi).

¹³⁶ *Id.* § 1836(b)(2)(B)(v), (b)(2)(F). Because the legislation is silent on the issue, presumably the court, in parallel with the seizure process, may entertain proceedings for more common forms of injunctive orders under Rule 65.

¹³⁷ 18 U.S.C.A. § 1836(b)(2)(B)(v), (b)(2)(F)(iii).

¹³⁸ *Id.* § 1836(b)(2)(D)(i)-(ii).

copies may be made.¹³⁹ On motion the court may order any electronic files to be encrypted.¹⁴⁰

Regarding the more prosaic aspects of a trade secret claim, the DTSA follows closely the language of the UTSA, changing somewhat the EEA definition of a “trade secret” to require that its value derive from not being known or accessible to “another person who can obtain economic value from the disclosure or use of the information.”¹⁴¹ In the section on remedies, the DTSA follows the UTSA language allowing for injunctions against “actual or threatened” misappropriation, but adds a significant limitation when the defendant is a departing employee intending to move to a competitor. Under the DTSA the court may not prevent the “person from entering into an employment relationship,” and it may place limitations on the employment (for example, requiring a delay or working in a different position) only based on evidence of behavior from which a threat of misappropriation may be inferred, “and not merely on the information the person knows.”¹⁴² This provision was intended to address concerns about employee mobility and the “inevitable disclosure doctrine,”¹⁴³ a subject that was raised in the professors’ letters and is discussed in more detail below.¹⁴⁴ Familiar language from the UTSA defines injunctions requiring affirmative actions and, in exceptional circumstances, imposing a reasonable royalty for no longer than use of the trade secret could have been prohibited.¹⁴⁵

Damages are to be calculated as provided under the UTSA, consisting of the plaintiff’s actual loss, together with any unjust enrichment not otherwise accounted for.¹⁴⁶ Willful and malicious misappropriation can trigger an award of double damages, plus attorney’s fees.¹⁴⁷ Also consistent with the

¹³⁹ *Id.* § 1836(b)(2)(B)(iii)(I).

¹⁴⁰ *Id.* § 1836(b)(2)(H).

¹⁴¹ *Id.* § 1839(3)(B). This change resolves an anomaly in the EEA as originally enacted. *See* Pooley, Lemley & Toren, *supra* note 52, at 191.

¹⁴² 18 U.S.C.A. § 1836(b)(3)(A)(i)(I). *Compare* UNIF. TRADE SECRETS ACT § 2(a) (NAT’L CONFERENCE OF COMM’RS ON UNIFORM STATE LAWS 1985), *with* Defend Trade Secrets Act (DTSA) of 2016, Pub. L. No. 114-153, § 2(a), 130 Stat. 376, 380 (to be codified at 18 U.S.C. § 1836(b)(3)(A)(i)(I)).

¹⁴³ *See* Seaman, *supra* note 11, at 365-67.

¹⁴⁴ Baker et al., *supra* note 9, at 5-6; Goldman et al., *supra* note 16, at 4-5; *see also* discussion *infra* Part VII.

¹⁴⁵ *Compare* UNIF. TRADE SECRETS ACT § 2(a)-(b) (NAT’L CONFERENCE OF COMM’RS ON UNIFORM STATE LAWS 1985), *with* DTSA § 2(a), 130 Stat. at 380 (to be codified at 18 U.S.C. § 1836(b)(3)(A)(ii)-(iii)).

¹⁴⁶ *Compare* UNIF. TRADE SECRETS ACT § 3(a) (NAT’L CONFERENCE OF COMM’RS ON UNIFORM STATE LAWS 1985), *with* DTSA § 2(a), 130 Stat. at 380 (to be codified at 18 U.S.C. § 1836(b)(3)(B)(i)).

¹⁴⁷ *Compare* UNIF. TRADE SECRETS ACT §§ 3(b), 4 (NAT’L CONFERENCE OF COMM’RS ON UNIFORM STATE LAWS 1985), *with* DTSA § 2(a), 130 Stat. at 380 (to be codified at 18 U.S.C. § 1836(b)(3)(C)-(D)).

UTSA, attorney's fees may be awarded to a defendant if a claim of misappropriation was prosecuted in bad faith.¹⁴⁸

The DTSA sets a limitations period of three years from discovery, which matches the UTSA, although it also shorter than the limitation period actually established by some state legislatures.¹⁴⁹ Significantly, given the EEA's special provisions defining criminal behavior, the DTSA adds a definition of "misappropriation" to § 1839 that tracks the language of the UTSA, but that also specifies that "improper means" may not include "reverse engineering or independent derivation," another concern that was highlighted by the professors' 2014 letter.¹⁵⁰

The legislation applies to any misappropriation "for which any act occurs on or after" its enactment.¹⁵¹ One curious provision declares that the DTSA "shall not be construed to be a law pertaining to intellectual property for purposes of any other Act of Congress."¹⁵² This apparently is a reference to section 509 of the Communications Decency Act of 1996, which protects Internet service providers and other republishers from liability, except in regard to laws "pertaining to intellectual property."¹⁵³ The logical dilemma of this expedient is apparent from the opening line of the Senate Judiciary Committee report on the bill, which flatly states that "[t]rade secrets are a form of intellectual property."¹⁵⁴ As already noted, the statute is expressly nonpreemptive, leaving the states free to continue to fashion and enforce their own laws relative to trade secrets.¹⁵⁵

Beyond adding a civil right of action, the DTSA amends the criminal provisions of the EEA. First, it changes the maximum fine imposed under 18 U.S.C. § 1832(b) from \$5 million to the greater of that amount or three

¹⁴⁸ Compare UNIF. TRADE SECRETS ACT § 4 (NAT'L CONFERENCE OF COMM'RS ON UNIFORM STATE LAWS 1985), with DTSA § 2(a), 130 Stat. at 380 (to be codified at 18 U.S.C. § 1836(b)(3)(D)).

¹⁴⁹ Compare UNIF. TRADE SECRETS ACT § 6 (NAT'L CONFERENCE OF COMM'RS ON UNIFORM STATE LAWS 1985), with DTSA § 2(a), 130 Stat. at 380 (to be codified at 18 U.S.C. § 1836(d)). Although most states have adopted the three-year period proposed by the UTSA, eight have not. Maine, Nebraska, Ohio, and Wyoming have adopted four years. ME. STAT. tit. 10, § 1547 (2015); NEB. REV. STAT. § 87-506 (2016); OHIO REV. CODE ANN. § 1333.66 (LexisNexis 2016); WYO. STAT. ANN. § 40-24-106 (2015). Georgia, Illinois, and Missouri designate five years. GA. CODE ANN. § 10-1-766 (2015); 765 ILL. COMP. STAT. 1065/7 (2016); MO. REV. STAT. § 417.461 (2015). And Vermont allows six years. VT. STAT. ANN. tit. 12, § 523 (2015).

¹⁵⁰ Baker et al., *supra* note 9, at 4. Compare UNIF. TRADE SECRETS ACT § 1(1)-(2) (NAT'L CONFERENCE OF COMM'RS ON UNIFORM STATE LAWS 1985), with DTSA § 2(b)(3), 130 Stat. at 380-81 (to be codified at 18 U.S.C. § 1839(5)-(6)) (excluding "any other lawful means of acquisition" from the definition of "improper means" in addition to excluding "reverse engineering" and "independent derivation").

¹⁵¹ DTSA § 2(e).

¹⁵² *Id.* § 2(g).

¹⁵³ Communications Decency Act of 1996, Pub. L. No. 104-104, sec. 509, § 230(d)(2), 110 Stat. 133, 139 (current version at 47 U.S.C. § 230(e)(2) (2012)).

¹⁵⁴ S. REP. NO. 114-220, at 1 (2016).

¹⁵⁵ DTSA § 2(f).

times the value of the stolen secret, including avoided costs of independent development.¹⁵⁶ Second, it adds a provision requiring that trade secret disclosures forced during a prosecution must be made under seal, for the protection of the owner, who does not thereby waive any rights in the information.¹⁵⁷

The law requires a biennial report on trade secret theft from the attorney general—working with the IP Enforcement Coordinator and the Director of the U.S. Patent and Trademark Office—describing enforcement in foreign jurisdictions, actions taken by U.S. agencies, and recommendations.¹⁵⁸ It requires that the Federal Judicial Center develop and submit “recommended best practices” relating to the provisions for ex parte seizure.¹⁵⁹ And it includes a statement of the “sense of Congress” that trade secret theft is an international problem that harms both companies and their employees.¹⁶⁰

Finally, the DTSA amends 18 U.S.C. § 1833 to establish immunity for employee whistleblowers, discussed in detail below.¹⁶¹

V. THE DTSA MEETS A REAL NEED FOR EFFECTIVE TRADE SECRET REMEDIES IN A GLOBAL, DIGITAL ECONOMY

Imagine or remember a time before the arrival of such technological wonders as smartphones, USB drives, and the Internet. In the 1970s and 80s, taking trade secrets from a business typically was slow and tedious work, involving standing at a photocopier at night and making hundreds or thousands of copies. And although misappropriation was, as it still is, most often committed by (or with the help of) insiders with permission to be in the facility, usually there was physical evidence (or a security camera) pointing to the perpetrator. The intended beneficiaries were typically a start-up or the local office of a domestic competitor. In short, trade secret thefts were mostly local affairs, and could be handled by local courts applying their states’ laws.

Now, return to the present and you will readily understand why this scene, only three decades distant, seems so impossibly quaint. With the arrival of ubiquitous digital devices with massive storage and robust wireless communications, the risk profile of holding trade secrets has been profoundly and irretrievably altered. Never have information assets been so

¹⁵⁶ *Id.* § 3(a)(1), 130 Stat. at 382 (to be codified at 18 U.S.C. § 1832(b)).

¹⁵⁷ *Id.* § 3(a)(2)(B), 130 Stat. at 382 (to be codified at 18 U.S.C. § 1835(b)).

¹⁵⁸ *Id.* § 4(b).

¹⁵⁹ *Id.* § 6(a).

¹⁶⁰ *Id.* § 5(1)-(2).

¹⁶¹ DTSA § 7(a), 130 Stat. at 384-85 (to be codified at 18 U.S.C. § 1833(a)-(b)); *see infra* Part VIII.

vulnerable to loss. And never have they been so valuable. As reported by Ocean Tomo, the share of public company value represented by intangible information leapt from 17 percent in 1975 to 68 percent in 1995 to 84 percent in 2015.¹⁶² This means that industry in the span of a single generation has experienced a shift of historic proportions in the kind of property it uses to create value.

In another important shift, the way that companies choose to protect their investment in their innovations has moved away from a concentration on patenting and towards trade secrets. This was first reported in 2000 by researchers at Carnegie-Mellon¹⁶³ and was confirmed by a 2012 report from the National Science Foundation and the Census Bureau.¹⁶⁴ They found that, among “R&D-intensive” firms—who collectively account for two thirds of U.S. R&D investment—secrecy was deemed important at more than twice the level of patents.¹⁶⁵

In recent years the headlines about cyberhacking have turned public attention toward the subject of trade secrets. But while these remote and stealthy attacks have caused extensive damage and properly raised concerns about safety of the nation’s information infrastructure, most corporate secrets are still lost, as they were thirty years ago, through insiders.¹⁶⁶ The difference today is that digital tools make this kind of misappropriation easier, cheaper, and harder to detect. More to the central point of the DTSA, they make disappearance of the stolen property simpler and faster. And the destination is less likely to be a start-up company in the neighborhood. If an employee—or accomplice of an employee—slips a DVD into a purse or a USB into a pocket, it may be a matter of days or even hours before the perpetrator boards a plane out of the country.

In short, the risk of trade secret misappropriation is now digital and global, and the remedies to address it have to match the risk. Viewed in that light, the enforcement situation faced by U.S. industry has been sadly inadequate. State laws are far from uniform, placing a burden on companies with regional or national operations.¹⁶⁷ This is not an abstract problem. Be-

¹⁶² Kristi L. Stathis, *Ocean Tomo Releases 2015 Annual Study of Intangible Asset Market Value*, OCEAN TOMO INSIGHTS BLOG (Mar. 5, 2015), <http://www.oceantomo.com/blog/2015/03-05-ocean-tomo-2015-intangible-asset-market-value/>.

¹⁶³ Wesley M. Cohen et al., *Protecting Their Intellectual Assets: Appropriability Conditions and Why U.S. Manufacturing Firms Patent (or Not)* (Nat’l Bureau of Econ. Research, Working Paper No. 7552, 2000), <http://www.nber.org/papers/w7552>.

¹⁶⁴ John E. Jankowski, *Business Use of Intellectual Property Protection Documented in NSF Survey*, NSF INFO BRIEF (Nat’l Science Found., Arlington, Va.), Feb. 2012, <http://www.nsf.gov/statistics/infbrief/nsf12307/nsf12307.pdf>.

¹⁶⁵ *Id.* at 3.

¹⁶⁶ *Can You Keep a Secret?*, ECONOMIST (Mar. 16, 2013), <http://www.economist.com/news/business/21573580-patent-idea-you-must-publish-it-many-firms-prefer-secrecy-can-you-keep-secret>.

¹⁶⁷ Identification of secrets in litigation is one example of a procedural issue unique to some states that can affect the progress of a misappropriation case. In California, no discovery by the plaintiff is

fore the DTSA, a trade secret owner who learned of an impending misappropriation in a location remote from its headquarters usually had to go to a county court, appearing before a motions judge sitting on a rotation system, or operating under local rules and customs that could limit or even deny direct access to the judge. And, if there was access, the judge was not likely to be very familiar with complex issues of comity and personal jurisdiction that are common to international disputes—and therefore could be reluctant to act.

But even where the boundaries are only between states, the pre-DTSA system was suboptimal. As any lawyer with relevant experience can confirm, the “need for speed” in an interstate trade secret case can seldom be satisfied through state court procedures. Mark Halligan, an experienced trade secrets litigator, describes the problem well:

Suppose the trade secrets case is pending in state court in Illinois and discovery establishes that a critical witness with potentially smoking-gun evidence resides in California. The first step required is the filing of a motion in Illinois state court requesting the Illinois court to issue a discovery petition authorizing the out-of-state deposition. After obtaining the Illinois court order, a special action must then be filed in California to obtain a court order from the California court under the doctrine of comity among states to authorize the valid issuance of the subpoena in California to the California resident. The whole process can take months with briefings both in the Illinois courts and the California courts.¹⁶⁸

It is no answer to suggest, as have Professors Levine and Sandeen, that federal prosecutors stand at the ready to take such cases to federal court under the pre-DTSA criminal provisions of the EEA.¹⁶⁹ The reality is starkly different, as described by former federal prosecutor Peter Toren, who has analyzed the relatively “languid pace” of filings (eight per year on average) under the statute.¹⁷⁰ As Mr. Toren points out, EEA investigations and prosecutions are “resource intensive and complex,” often requiring technical expertise that prosecutors do not possess, and as a result they are inclined to exercise their discretion to refuse the case in favor of handling other matters.¹⁷¹ This “reluctance to prosecute EEA cases is reinforced” by internal guidelines that disfavor prosecution when the victim has a civil remedy, as most do.¹⁷²

In short, the time-critical nature of interstate and international misappropriation of valuable digitized data requires an immediate and sophisticated response mechanism, and neither state law nor the EEA criminal framework offers a satisfactory solution. Federal courts, however, can pro-

permitted until the plaintiff has described the relevant secrets at a level of detail (“reasonable particularity”) that satisfies the court. CAL. CIV. PROC. CODE § 2019.210 (West 2005).

¹⁶⁸ See Halligan, *supra* note 61, at 494 (footnotes omitted).

¹⁶⁹ See Levine & Sandeen, *supra* note 11, at 249-50, 254.

¹⁷⁰ See Toren, *supra* note 54.

¹⁷¹ *Id.*

¹⁷² *Id.*

vide the necessary resource. First, they will be operating under a single, national standard for trade secret misappropriation and a transparent set of procedural rules, offering a much-needed level of predictability and ease of use. Second, they provide nationwide service of process and a unified approach to discovery, enabling quick action by trade secret owners even when confronted with actors in multiple jurisdictions.¹⁷³ Third, as a result of their extensive experience with complex cross-border litigation involving intellectual property, they will be able to resolve *ex parte* matters fairly and jurisdictional issues quickly and efficiently. Fourth, their generally more predictable and uniform discovery procedures will serve the legitimate needs of trade secret plaintiffs, who typically must develop most of the facts to prove their case through defendants and third parties.¹⁷⁴

Having reliable access to federal courts in trade secret cases requires the original jurisdiction offered by the DTSA. It is not sufficient to say that plaintiffs can enter the federal system through diversity jurisdiction, as complete diversity is required, and many trade secret cases do not qualify due to the involvement of one or more local defendants. And supplemental jurisdiction is not the answer either, as not all cases present the opportunity to plead a claim based on federal law, and, in any event, the decision to exercise supplemental jurisdiction depends on finding a common core of facts.¹⁷⁵

VI. THE SEIZURE REMEDY IS NARROWLY DRAWN TO A SPECIFIC NEED

As already discussed, modern digital technology has made trade secrets more vulnerable to loss.¹⁷⁶ When a company discovers that valuable information is in the possession of a rogue employee and evidence clearly demonstrates that he is likely to destroy it or flee the jurisdiction with it, the owner deserves access to a prompt and effective remedy to prevent irreparable harm. Even before the DTSA, the remedy of *ex parte* seizure was not unknown in federal cases dealing with trade secrets, as FRCP Rule 65(b) allows orders to be entered without notice when specific facts are provided to demonstrate the immediacy of the harm and the reasons why notice

¹⁷³ See Halligan, *supra* note 61, at 493-94.

¹⁷⁴ See *Greenberg v. Croydon Plastics Co.*, 378 F. Supp. 806, 814 (E.D. Pa. 1974) (“Plaintiffs in trade secret cases, who must prove by a fair preponderance of the evidence disclosure to third parties and use of the trade secret by the third parties, are confronted with an extraordinarily difficult task. Misappropriation and misuse can rarely be proved by convincing direct evidence. In most cases plaintiffs must construct a web of perhaps ambiguous circumstantial evidence from which the trier of fact may draw inferences which convince him that it is more probable than not that what plaintiffs allege happened did in fact take place. Against this often delicate construct of circumstantial evidence there frequently must be balanced defendants and defendants’ witnesses who directly deny everything.”).

¹⁷⁵ See *supra* note 119 and accompanying text.

¹⁷⁶ See *supra* note 162 and accompanying text.

should not be required.¹⁷⁷ The DTSA preserves these conditions and goes well beyond Rule 65(b) in prescribing other conditions and restrictions, ensuring that orders are available only under “extraordinary circumstances” and only to “prevent the propagation or dissemination of the trade secret.”¹⁷⁸

But allowing an ex parte seizure is categorically unacceptable to the authors of the *Trolls* article, who suggest instead that the victimized business should use its rights under existing law to “search company premises, requiring the return of company property, or engag[e] in timely exit interviews.”¹⁷⁹ Such self-help measures can work well in an environment where the departing employee is cooperative, but in more hostile situations they are utterly impractical. The same is true for the authors’ proposed solution that “larger and more sophisticated companies” can place a “legal hold” on their records in anticipation of litigation.¹⁸⁰ But the most unfathomable of the authors’ arguments on this point is that destruction of records is actually “beneficial to the trade secret owner to the extent it eliminates the threat of wrongful disclosure or use of the information.”¹⁸¹ This sort of reasoning not only trivializes a serious wrong but also invites a new and dangerous perspective on spoliation of evidence.

While our court system must provide a realistic ex parte remedy to prevent prospective catastrophic loss of information assets, the remedy should be drawn narrowly, to permit intervention only to the extent required, with appropriate disincentives against abuse. The DTSA strikes that balance well. In the first place it demands compelling proof of a real risk of disappearance or destruction of the trade secrets.¹⁸² From the sworn affidavit it must “clearly appear” that a restraining order under Rule 65(b)—for example, an order preventing destruction or removal from the jurisdiction—would be ineffective because “specific facts” demonstrate that the defendant “would evade, avoid, or otherwise not comply with such an order.”¹⁸³ The plaintiff’s abstract fear—for example, one based on the defendant’s access to the information and its easily transportable character—will not be enough.¹⁸⁴ Instead, judges will have to see clear evidence of relevant behavior, such as excessive downloading followed by reformatting of the company laptop, revenge-tainted threats, missing files, attempted, improper access to data, and the like, which when considered in context convinces the court that the secrets are in immediate peril.

¹⁷⁷ Cf. *First Tech. Safety Sys., Inc. v. Depinet*, 11 F.3d 641, 652 (6th Cir. 1993) (reversing a district court seizure order where facts were insufficiently specific to justify ex parte relief).

¹⁷⁸ 18 U.S.C.A. § 1836(b)(2)(A)(i) (West 2016).

¹⁷⁹ See Levine & Sandeen, *supra* note 11, at 253.

¹⁸⁰ *Id.* (internal quotation marks omitted).

¹⁸¹ *Id.*

¹⁸² 18 U.S.C.A. § 1836(b)(2)(A)(ii).

¹⁸³ *Id.* § 1836(b)(2)(A)(ii)(I).

¹⁸⁴ See *First Tech. Safety Sys., Inc. v. Depinet*, 11 F.3d 641, 652 (6th Cir. 1993).

This statutory framework is not new; it has been used in the field of counterfeit goods.¹⁸⁵ The Lanham Act provisions for ex parte seizure are an obvious predecessor, allowing the remedy only where it “clearly appears from specific facts” that another kind of order would not suffice.¹⁸⁶ The parallels continue with requirements for specific findings supporting a balance of harm in favor of the proponent due to an imminent danger of irreparable harm and that the court hold the seized material and prevent publicity of the proceedings.¹⁸⁷

The DTSA requirements for trade secret seizure are significantly more stringent than those in the Lanham Act. The order must minimize interruption to the defendant’s legitimate business and avoid any disruption to other businesses, to prevent collateral damage.¹⁸⁸ And, while the Lanham Act allows a hearing to be set from ten to fifteen days later, the DTSA imposes a strict seven-day limit for holding a hearing.¹⁸⁹ During that time the defendant is free to make an application to dissolve or modify the seizure order.¹⁹⁰ Special provisions protect the integrity of information, by prohibiting copies, prohibiting connection to a network, restricting access, and allowing encryption.¹⁹¹

When considering the possibility of abuse by the applicant, one has to recognize not only the difficulty of making the case but also the penalties for not getting it right. The plaintiff must post a bond, but the bond will not limit the amount that the defendant and others affected by the order may claim for damages.¹⁹² Moreover, federal judges are not known for suffering fools gladly, and they have substantial powers to sanction inappropriate behavior under FRCP Rule 11.¹⁹³ What plaintiff—or plaintiff’s counsel—would take that sort of open-ended risk for a few days of inconvenience meted out to a former employee or competitor? And, if the claim is truly and obviously meritless, why would a defendant “capitulate,” rather than just file an opposition?

The authors of the *Trolls* article argue that, in spite of all the restrictions, the potential for abuse remains because a trade secret owner

¹⁸⁵ Internationally, the comparable “*Anton Piller* seizure order” has been regularly used in the United Kingdom and Canada. See, e.g., *Celanese Canada Inc. v. Murray Demolition Corp.*, [2006] 2 S.C.R. 189 (Can.); *Anton Piller K.G. v. Mfg. Processes Ltd.*, [1975] EWCA (Civ) 12 (Eng.).

¹⁸⁶ 15 U.S.C. § 1116(d)(4)(B) (2012).

¹⁸⁷ *Id.* § 1116(d)(5)-(7).

¹⁸⁸ 18 U.S.C.A. § 1836(b)(2)(B)(ii) (West 2016).

¹⁸⁹ *Id.* § 1836(b)(2)(B)(v).

¹⁹⁰ *Id.* It is therefore difficult to comprehend how the authors of the professors’ 2015 letter could assert that “an alleged misappropriator will be unable to immediately and meaningfully challenge the plaintiff’s assertions” in an ex parte application. See Goldman et al., *supra* note 16, at 3. There is no reason that the defendant could not mount such a challenge the same day or the next.

¹⁹¹ 18 U.S.C.A. § 1836(b)(2)(B)(iii)(I), (b)(2)(D)(i)-(ii), (b)(2)(H).

¹⁹² *Id.* § 1836(b)(2)(B)(vi).

¹⁹³ FED. R. CIV. P. 11.

could exact a settlement payment by sending out letters threatening an ex parte seizure application.¹⁹⁴ But the argument immediately collapses under its own weight. The entire purpose of making an application ex parte is to avoid notice, in order to prevent behavior that could happen if notice were given. It makes no sense to suggest that an ex parte process could be abused by threatening to invoke it.

VII. THE DTSA PROVIDES A SENSIBLE APPROACH TO “THREATENED MISAPPROPRIATION” INJUNCTIONS AGAINST DEPARTING EMPLOYEES

The professors’ 2014 letter claimed that the previous draft legislation would “limit mobility of labor,”¹⁹⁵ but did not explain exactly why this was so. In the articles published since, the contours of the argument began to emerge. Professor Argento built her position on the assumption that “trade secret rights are intended to serve the public interest, not trade secret holders specifically.”¹⁹⁶ This was a novel reinterpretation of the rationale laid down by the Supreme Court in *Kewanee Oil*, which recognized the twin policy objectives of enforcing commercial morality and encouraging innovation. Naturally, the public benefits indirectly from ethics in business and from the innovative work of industry. But the immediate beneficiary of trade secret law is the one holding the secret because, without the law’s support, the holder (in particular a small business) would be harmed by expensive and inefficient self-help measures deployed to keep information secret.¹⁹⁷ From her public-interest-centered position, Professor Argento argued that departing employees can serve society through a “cross-pollination effect,” resulting from “seepage of useful information that benefits the public.”¹⁹⁸

The Seaman article developed the point further by invoking the so-called “inevitable disclosure doctrine,” a subject that gained prominence (or notoriety, depending on your point of view) following a court ruling that prohibited an executive from taking the same job with a direct competitor because the circumstances indicated a threat of disclosure or use of the secrets he knew.¹⁹⁹ Using “inevitable disclosure” as an example, Professor

¹⁹⁴ See Levine & Sandeen, *supra* note 11, at 255 (arguing that, before the court could act on an application, “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 . . . 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 devastated based upon an unproven allegation or a seizure remedy improperly issued.”).

¹⁹⁵ See Baker et al., *supra* note 9, at 6.

¹⁹⁶ See Argento, *supra* note 11, at 202.

¹⁹⁷ See *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 485-86 (1974).

¹⁹⁸ See Argento, *supra* note 11, at 188.

¹⁹⁹ *Pepsico, Inc. v. Redmond*, 54 F.3d 1262, 1272 (7th Cir. 1995).

Seaman argued that federalizing trade secret law could endanger free movement of labor by removing the states' ability to serve as "laboratories" for competing policy positions.²⁰⁰ He forecast the result that "firms that engage in innovation protected by trade secrecy would no longer be free to choose whether to conduct their research in states that follow (or do not follow) the inevitable disclosure doctrine."²⁰¹

The professors' 2015 letter went further, arguing that the new version of the DTSA "implicitly recognize(s)" the doctrine, which it claims can "prevent individuals from being able to feed their families."²⁰² In fact, the specific language begins with a provision taken directly from the UTSA, which, as already noted, authorizes injunctions to prevent "actual or threatened misappropriation."²⁰³ The DTSA as originally drafted added this proviso: "provided the order does not prevent a person from accepting an offer of employment under conditions that avoid actual or threatened misappropriation."²⁰⁴ The intent was that courts be able to set reasonable conditions on employment, in order to avoid circumstances that would threaten the integrity of secret information. But the proviso also seemed to trigger a focus on the assumed evil of the abstract "doctrine." This is unfortunate, since there is much less to the doctrine than meets the eye.

To understand this we need to return to the Seventh Circuit decision in *Pepsico, Inc. v. Redmond*,²⁰⁵ affirming a five-month injunction against a former marketing executive who had lied about his plans to take an identical position with another company that was about to launch a directly competitive product.²⁰⁶ Although the court had emphasized the executive's bad behavior, it also summarized that "defendant's new employment will inevi-

²⁰⁰ See Seaman, *supra* note 8, at 365-66.

²⁰¹ *Id.* at 367. Professor Seaman's fears are not grounded in fact. The new law is not preemptive, leaving state legislatures and courts free to experiment on any issues that they deem important. Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, § 2(f), 130 Stat. 376, 382. Thus, although there is no evidence of any company actually choosing to locate its R&D facilities based on local acceptance or rejection of inevitable disclosure, nothing in the bills would foreclose that hypothetical possibility.

²⁰² See Goldman et al., *supra* note 16, at 5. The professors support their concern with citation to a paper arguing "that lesser constraints on employee mobility may increase economic growth and innovation." *Id.* (quoting On Amir & Orly Lobel, *Driving Performance: A Growth Theory of Noncompete Law*, 16 STAN. TECH. L. REV. 833, 837-38 (2013)) (internal quotation marks omitted). The authors of that paper describe an online survey experiment suggesting that employees perform less well when they know they will be prohibited from doing the same task later or will be paid less to do it. Amir & Lobel, *supra*, at 854. Apart from the question of how much can be extrapolated from the observation that people are more productive when they know they are free to do what they like afterwards, the paper begs the very important question of how much of that value should be set off against the loss of valuable rights when employees decide to leave with otherwise protectable secrets.

²⁰³ UNIF. TRADE SECRETS ACT § 2(a) (NAT'L CONFERENCE OF COMM'RS ON UNIF. STATE LAWS 1985).

²⁰⁴ S. 1890, 114th Cong. § 2(a) (2015).

²⁰⁵ 54 F.3d 1262 (7th Cir. 1995).

²⁰⁶ *Id.* at 1264, 1272.

tably lead him to rely on the plaintiff's trade secrets."²⁰⁷ Commentators promptly wrenched this dictum from its context and warned that *Pepsico* could be used to justify enjoining someone from taking a job only because of what he or she knew. This is how the so-called "inevitable disclosure doctrine" was born.

Having (mis)construed *Pepsico* this way, it was easy to make it a target, raising the alarm that "inevitable disclosure" was the equivalent of a post-hoc judicially-imposed noncompetition agreement.²⁰⁸ Perhaps unsurprisingly, the backlash was particularly strong in California, which values its statutory prohibition against contracts restraining individuals from "engaging in a lawful profession, trade, or business."²⁰⁹ In *Whyte v. Schlage Lock Co.*,²¹⁰ an intermediate appellate court issued a blistering condemnation of the doctrine and flatly declared it unacceptable under California law.²¹¹ It did this in response to the plaintiff's argument that the doctrine should be available as an "alternative" to proving "threatened misappropriation." Just what kind of evidence might be enough to establish a threat under the UTSA was not addressed. However, that question was answered several years later by another California court in *Central Valley General Hospital v. Smith*.²¹² It explained that evidence of bad behavior, such as a prior misappropriation, an intention to misappropriate, or a refusal to return confidential material, should be enough to supply the inference.²¹³

In the meantime, however, the ideological battle lines had been drawn, and the forces mustering against inevitable disclosure, reinforced by many academic and popular articles, were determined to stamp it out if possible, or at least to protect their own jurisdiction from infection. The fervor of the debate apparently distracted everyone from critically examining what "inevitable disclosure" meant, or how it was actually being applied in places that didn't have a reflexive opposition to it. In fact, there is very little evidence of its being used as the opponents assumed, that is where the only threat indicator was how much the employee knew. This led some of us who were engaged in negotiations over the DTSA to try reframing the question in terms from the established language of the UTSA: just what kind of evidence should be used to infer "threatened" misappropriation by a depart-

²⁰⁷ *Id.* at 1269.

²⁰⁸ *See, e.g.,* Seaman, *supra* note 11, at 367 n.337 (quoting Elizabeth A. Rowe, *When Trade Secrets Become Shackles: Fairness and the Inevitable Disclosure Doctrine*, 7 TUL. J. TECH. & INTELL. PROP. 167, 183 (2005)).

²⁰⁹ CAL. BUS. & PROF. CODE § 16600 (West 2005).

²¹⁰ 125 Cal. Rptr. 2d 277 (Cal. Ct. App. 2002).

²¹¹ *Id.* at 293 ("Lest there be any doubt about our holding, our rejection of the inevitable disclosure doctrine is complete.")

²¹² 75 Cal. Rptr. 3d 771 (Cal. Ct. App. 2008).

²¹³ *Id.* at 792.

ing employee?²¹⁴ The answer most consistent with logic, evidence law, and sensible public policy is that the employee's behavior demonstrating unreliability, rather than how much he or she knows, should inform the court's conclusion.

In the end, Senator Feinstein offered an amendment reflecting this approach, clarifying that an injunction may not "prevent a person from entering into an employment relationship," and that any conditions imposed on taking the job "shall be based on evidence of threatened misappropriation and not merely on the information the person knows."²¹⁵ In a belt-and-suspenders approach, the DTSA also includes a directly related amendment proposed by Senator Cornyn that the order may not "otherwise conflict with an applicable State law prohibiting restraints on the practice of a lawful profession, trade, or business."²¹⁶

VIII. WHISTLEBLOWER IMMUNITY IS OVERDUE BUT APPROPRIATELY NARROW

Senators Leahy and Grassley offered a separate, second major amendment to the DTSA, addressing a long-neglected question in trade secret law: how do we assure that employees who come upon evidence of illegal activity, but who are constrained by nondisclosure agreements from communicating those facts, can safely speak to their lawyers and to law enforcement officials? One might think that this question would already have been reliably answered by now, but before the DTSA it was largely ignored. In a wide-ranging and thoughtful article on the subject, *Tailoring a Public Policy Exception to Trade Secret Protection*,²¹⁷ Professor Peter Menell of the UC Berkeley Law School explored not only the sparse, murky, and sometimes-contradictory legal authority, but also the psychology of whistleblowing and the importance of a clear "safe harbor" for those who are thinking of reporting wrongdoing. As a practical matter, employees and contractors face a stark dilemma, where the upside is a clear conscience (and possibly a reward for uncovering fraud) but the downside can involve

²¹⁴ The author wishes to thank Professor Mark Lemley of Stanford Law School for his collaboration and insights in helping craft this proposal.

²¹⁵ S. 1890, 114th Cong. (as amended by substitute, Jan. 28, 2016), http://www.judiciary.senate.gov/download/s1890-substitute-amendment_-ehf16041 (including Sen. Feinstein's language); S. REP. NO. 114-220, at 8 (2016) ("[S]ome members, including Senator Feinstein, voiced concern that the injunctive relief authorized under the bill could override state-law limitations that safeguard employee mobility . . ."); see also 18 U.S.C.A. § 1836(b)(3)(A)(i)(I) (West 2016).

²¹⁶ S. 1890, 114th Cong. (as amended by substitute, Jan. 28, 2016), http://www.judiciary.senate.gov/download/s1890-substitute-amendment_-ehf16041 (including Sen. Cornyn's language); see also 18 U.S.C.A. § 1836(b)(3)(A)(i)(II).

²¹⁷ Peter S. Menell, *Tailoring a Public Policy Exception to Trade Secret Protection* (Jan. 3, 2016) (unpublished manuscript), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2686565.

painful and relentless retaliation as well as personal, financial, legal, and professional risk. Insulating the whistleblower from costly trade secret exposure would serve larger societal interests in law enforcement, tax compliance, and surfacing and deterring securities fraud and fraud against the government.

Yet because of the difficulty of enforcing trade secrets once they leak, companies risk potentially significant losses if employees or contractors mistakenly disclose legitimate trade secrets—i.e., those that do not reveal illegal conduct. Professor Menell's article provided an effective solution to this dilemma, by insulating whistleblowers and their counsel from liability for disclosing trade secret information *in confidence* to government officials or as part of a lawsuit alleging retaliation by an employer provided that the information is filed under seal.²¹⁸ His proposed statutory exception to trade secret liability would assure potential whistleblowers that they do not violate their NDAs merely by consulting legal counsel to report suspected illegal conduct to the government through a confidential channel.

The article appeared early in the process of Senate consideration of the bill. Senate staff reached out to Professor Menell to help craft appropriate language. As a result, Section 7²¹⁹ was added to the DTSA, providing immunity under federal or state law²²⁰ against any claim for violation of an individual's nondisclosure obligations for disclosure, made in confidence, to (a) an attorney or government official, for the purpose of reporting or investigating a violation of law, or (b) a filing made under seal in a lawsuit "or other proceeding." In order to ensure that employees (a term that also includes contractors and consultants) know about their rights, employers are required to give an appropriate notice in the nondisclosure agreement (as is often done now with state inventor statutes), although this can be a reference to the company's separate policy document.²²¹ A failure to comply with the notice provision would block any award of attorneys' fees or enhanced damages against an employee under the DTSA. Significantly, whistleblower immunity does not extend to any otherwise improper acts by the employee, such as hacking information in violation of the Computer Fraud and Abuse Act.²²²

²¹⁸ *Id.* at 69.

²¹⁹ Amendment to S. 1890, 114th Cong. (as proposed by Sens. Leahy and Grassley, Jan. 28, 2016), http://www.judiciary.senate.gov/download/s1890-leahy-grassley1_-alb16037 (adding language that would become section 7 of the DTSA to be codified at 18 U.S.C. § 1833).

²²⁰ In this narrow sense the DTSA can be said to preempt state law.

²²¹ 18 U.S.C.A. § 1833(b)(3)(A)-(B) (West 2016).

²²² *See id.* § 1833(b)(5).

IX. THE CONCEPT OF “TROLLS” CANNOT APPLY TO TRADE SECRETS

The term “trade secret troll” is an oxymoron. As in the fairy tale where he controls access to an important bridge, the troll has to have the power to stop all unsuspecting pedestrians. Patents fill the bill, but trade secrets cannot. Just imagine the “trade secret troll” jumping up to file a lawsuit against a passer-by. The troll has to allege that the person participated in either a theft or a breach of confidence. There is no such thing as a no-fault trade secret claim.²²³ Anyone that might try to bundle them to build a business—for example, by sending out threat letters to an entire industry—is doomed to immediate failure.

This is a reflection of the profound differences between patents and secrets. Patents are granted by a government with the effect of excluding all others from making or selling the described invention. Liability is strictly imposed. Trade secret rights, in contrast, are not a government grant but derive from a private relationship in which information is shared in confidence. The law intervenes only when that specific confidence has been breached or an unauthorized actor has gained access by “improper means,” which the UTSA defines through the examples of “theft, bribery, misrepresentation, . . . or espionage.”²²⁴ Apart from that protection against misappropriation, the trade secret holder has no rights at all. Anyone else may hold the same information through independent discovery or reverse engineering of a publicly available product. This is why the Supreme Court called trade secrets “weak” relative to patents.²²⁵

The DTSA does not alter these fundamental facts, nor does it reduce any of the sanctions that have typically been applied to discourage frivolous claims.²²⁶ Apart from providing a very circumscribed and risky opportunity

²²³ The so-called “innocent misappropriator” who receives information unaware that it is someone else’s trade secret will face liability only prospectively from the time of receiving notice. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 cmt. d (1995); UNIF. TRADE SECRETS ACT §§ 2(b), 3(a) (NAT’L CONFERENCE OF COMM’RS ON UNIF. STATE LAWS 1985).

²²⁴ UNIF. TRADE SECRETS ACT § 1(1) (NAT’L CONFERENCE OF COMM’RS ON UNIF. STATE LAWS 1985). Another important distinction from patents, not specifically relevant to this point, is that trade secrets rights flow with the information across borders and are nominally enforceable wherever jurisdiction over the breach has been established. *See Seaman, supra* note 11, at 368. The enforceability of trade secrets is “nominal” because the enforcement of trade secret rights in other countries, although strongly influenced by Article 39 of the TRIPS Agreement, is quite variable. *See generally* Douglas C. Lippoldt & Mark F. Schultz, Org. for Econ. Co-operation & Dev. [OECD], *Uncovering Trade Secrets – An Empirical Assessment of Economic Implications of Protection for Undisclosed Data*, OECD Trade Policy Papers No. 167 (2014).

²²⁵ *See Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 489-90 (1974).

²²⁶ The law allows fee shifting for bringing a claim of misappropriation in “bad faith,” using exactly the same language as the UTSA. 18 U.S.C.A. § 1836(b)(3)(D). If “trade secret trolls” have not sprung to life in any of the forty-eight states that have established this negative incentive, why would anyone

to request *ex parte* seizure, as described above, the only major change wrought by the DTSA is to give trade secret holders the option of going directly to federal courts with their claims. What is it about that relatively modest change to the law that would provoke the appearance of a kind of litigant that has never been seen before in any of the states where trade secret laws have been enforced for over a century? One would assume that the proponents of such a scenario would have to come armed with real evidence combined with very persuasive logical analysis. Instead, they have provided only opinion (e.g., “the capabilities of trade secret trolls remain to be seen, but the risk is very real”)²²⁷ and apocalyptic speculation (e.g., “trade secret trolls [will] 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”).²²⁸

CONCLUSION

The Defend Trade Secrets Act meets a compelling need for effective protection of information assets in the digital age. The specific changes to the law are relatively modest and procedural. Its language draws from existing statutes. It does not preempt state legislation or policies. Instead, it offers a choice of federal forum and a remedy commensurate with the risks faced by modern businesses that compete on a global stage.

Our national economy depends increasingly on intangible assets, and businesses, large and small, use trade secret law more than any other kind of intellectual property law to protect those assets. At the same time, technology has exposed industrial secrets to unprecedented levels of risk. It only makes sense that creators and owners have now been given the same access to federal courts that they have enjoyed for their other intellectual property.

imagine that it would be easier to get a frivolous case past a federal judge, who also can impose sanctions under FRCP Rule 11?

²²⁷ See Levine & Sandeen, *supra* note 11, at 235.

²²⁸ *Id.* at 252.