Testimony of James Pooley
"Protecting Trade Secrets: the Impact of Trade Secret Theft on American Competitiveness and Potential Solutions to Remedy This Harm"
United States Senate Committee on the Judiciary
December 2, 2015

Introduction

Good morning Chairman Grassley, Ranking Member Leahy, and Members of the Committee. My name is James Pooley. I started my career as a lawyer in Silicon Valley in 1973, and over the course of the next 37 years I handled hundreds of trade secret disputes, including trials, arbitrations and settlements, in state and federal courts throughout the country. My clients were mostly smaller companies and individuals in the technology industry, and although I acted for both plaintiffs and defendants, most of the time I was on the defense side. I have tried to integrate my practical experience in intellectual property with an interest in scholarship and public policy. My legal treatise "Trade Secrets" has been updated semiannually since 1997, and for many years I taught trade secret law and litigation as an adjunct professor at the University of California, Berkeley and at Santa Clara University. My first business book about secrets was published in 1982 and my most recent one, *Secrets: Managing Information Assets in the Age of Cyberespionage*, was released earlier this year.

Thank you for holding this hearing and for inviting me to testify. Trade secret protection does not always get the same attention as other forms of intellectual property, and this hearing is therefore an important examination. It also comes at an important time, as the reliance on trade secret protection is increasing and the need for a federal civil remedy is becoming more apparent.

The views I express today are my own. My interest in these proceedings is only to provide a perspective informed by four decades of experience and study in how trade secrecy actually works for business and how trade secret disputes are resolved in state and federal courts.

As others have already pointed out to this Committee, information assets have rapidly come to form the core of our country's economy. As recently as the late 1970s, only twenty percent of public company value was represented by "intangibles." Today the number is over eighty percent. So in a single generation we have seen a shift of historic proportions in the nature of industrial property.

And that new property that fuels our economy is mainly protected as trade secrets. In a recent survey by the National Science Foundation and the Census Bureau, companies classified as "R&D-intensive" – which collectively account for 75% of private R&D spending in the U.S. – were asked to rank the importance of various kinds of IP laws in protecting their competitive advantage. Trade secrets

came out on top, rated at more than twice the level of patents.[1] This is particularly true for small businesses, which traditionally rely on simple secrecy much more than costly patents.

Trade secret theft hurts all kinds of companies, as well as our economy. When large companies lose secrets to a foreign competitor, the competitor can go straight to manufacturing without the costs and risks of honest R&D, allowing it to undercut the U.S. company, which loses profits and jobs. And things can be much worse for a small business that relies on a single line of products. When it loses the technology that gives it a competitive edge, it may have to shut down.

To maintain legal protection, companies have to take reasonable steps to keep their information secret. When I first started working in this area, information security was fairly simple: all a company had to do was guard the photocopier and watch who went in and out the front door of the building. Since then, advances in electronics like flash drives and smartphones have made data theft almost infinitely easier and faster. The new environment enables not just external hacking of corporate networks, but also misappropriation by trusted insiders like employees, consultants and suppliers. And unlike the threats of a generation ago, when trade secret theft typically benefited a local competitor, the globalization of business means that today's insiders often steal on behalf of companies located in other states or countries.

So within the time since I began my professional career, our economy has transformed to near-complete reliance on information for competitive advantage, while at the same time we have invented technologies that make it easier to steal that information and move it quickly out of the country. Traditional state remedies for trade secret misappropriation are too inefficient to fully meet this existential challenge. A complete solution requires the jurisdictional scope and special resources of federal courts.

Background of Trade Secret Law

U.S. trade secret law emerged in the nineteenth century to accommodate the shift from agrarian and cottage production to larger-scale industry, in which the secrets of production had to be shared with workers or business partners. Court decisions sought to enforce the confidence placed in those who were given access to valuable information about machines, recipes and processes. At the core of every case was a confidential relationship. Protecting this trust, the courts explained, was a simple matter of enforcing morality in the marketplace.

The common law origins of trade secrets – in contrast to the federal patent statute – meant that the majority of cases were heard in state court. Even when

---

[1] *Business Use of Intellectual Property Protection Documented in NSF Survey*, NSF 12-307 (2012), available at http://www.nsf.gov/statistics/infbrief/nsf12307/.

there was a special basis for jurisdiction, such as diversity of citizenship or a separate federal question, federal courts applied state common law. And at first there was little variation, with most states looking to the Restatement of Torts § 757 as a guide. But as industrial development continued through the middle of the twentieth century, legal foundations shifted, and the reporters of the Second Restatement dropped the subject completely.

Meanwhile, a school of thought had developed among commentators that trade secret law should be abolished altogether because it was inconsistent with, and therefore preempted by, federal patent law. This argument was famously rejected by the U.S. Supreme Court in *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470 (1974). Two important public interests, the Court explained, were served by trade secret law: the "maintenance of standards of commercial ethics and the encouragement of invention." 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. And as a practical matter, there was 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 "weaker," because they do not protect against reverse engineering or independent development.

The Uniform Trade Secrets Act Has Failed to Produce Needed Uniformity

By the time of the *Kewanee* decision, U.S. commerce was increasingly interstate and global. Some leaders in the IP community voiced concern that trade secret law would become too fractured and inconsistent for modern business. Therefore, in 1979 the National Conference of Commissioners on Uniform State Laws issued the first of two versions of the Uniform Trade Secrets Act ("UTSA"), proposing harmonized rules on establishing and enforcing trade secret rights.[2] Measured by adoption rates, the UTSA has been a great success, with 47 of the 50 states so far embracing it. However, measured by its objective of uniformity, the law has been a disappointment, because so many states have decided to deviate from the uniform text and customize their own version.

A few examples will help illustrate the scope of the problem. California dropped the language requiring that a trade secret be not "readily ascertainable," with the result that the defendant is required to specially plead that circumstance as an affirmative defense. Illinois also eliminated the "readily ascertainable" language, and it prohibits royalty injunction orders, sets a different limitations period and allows permanent injunctions. Idaho requires that computer programs carry a "copyright or other proprietary or confidential marking" to qualify for protection. Georgia limits protection of customer lists to physical embodiments, in effect

---

[2] Unif. Trade Secrets Act, available at http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf.

allowing employees to appropriate such information in (human) memory. South Carolina's version of the UTSA requires a court hearing an injunction request to consider "average rate of business growth" in determining the length of an injunction, and prescribes very particular rules for discovery of trade secret information.[3]

The problem is not just variations in trade secret law from state to state. Dealing with information theft in the modern world runs up against procedures that were not designed for efficiency in resolving cross-border litigation. If a case in Illinois requires testimony of a witness in California, the plaintiff has to petition its home court to authorize a deposition, and then file an action in California based on the Illinois order, to secure the required subpoena. During the weeks or months of this process, the witness could easily have left the country, with the secrets in her pocket.[4] Clearly, U.S. businesses cannot adequately address the full scope of modern threats to their trade secrets by filing litigation in state court.

Existing Federal Laws Cannot Solve the Problem

Civil claims for trade secret misappropriation can sometimes be brought in federal court, but only in two limited situations. First, if another claim exists under federal law, such as patent infringement, then a related trade secret claim can be asserted in the same case, but only if it is based on the same central set of facts as the federal claim.[5] This is no help to the business owner facing the classical problem of an employee leaving with the company's secrets, because usually there is no other federal law that can be applied to the case. Second, if the theft is in service of an out-of-state competitor, it may be possible to get into federal court with a state law claim by asserting diversity of citizenship. But in the typical case where the departing employee is a local resident, this can't work because diversity has to be "complete," and the presence of any local defendant will defeat the claim.[6]

---

[3] For a comprehensive collection of state variations, see Sid Leach, *Anything but Uniform: A State-By-State Comparison of the Key Differences in the Uniform Trade Secrets Act* (2015) available at 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

[4] See 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, 494 (2015).

[5] See 28 U.S. C. §1367; United Mine Workers of America v. Gibbs, 383 U.S. 715, 725 (1966); Tech Enterprises, 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).

[6] Lincoln Property Co. v. Roche, 546 U.S. 81, 82 (2005).

Another option may be to ask the U.S. Attorney to bring criminal charges under the Economic Espionage Act ("EEA").[7] But because of limited prosecutorial resources and a higher burden of proof, only a fraction of deserving cases can be accepted. And many companies decline to pursue criminal remedies because of the required surrender of control or the effects on a concurrent civil claim of the defendant's assertion of a Fifth Amendment privilege.[8] Although the EEA provides potentially powerful remedies, it is unrealistic to expect the underlying problem to be solved comprehensively by a criminal statute.

In other words, 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 provides a satisfactory solution. Federal courts, however, can provide the necessary resource. First, under the DTSA federal courts would operate under a single, national standard for trade secret misappropriation and a transparent set of procedural rules, offering predictability and ease of use. Second, federal courts 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. Third, as a result of their extensive experience with complex cross-border litigation involving intellectual property, federal courts would be able to resolve jurisdictional issues quickly and applications for injunctions or seizures fairly. Fourth, their generally more predictable 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.

The Defend Trade Secrets Act and the Law Professors' Opposition

The Defend Trade Secrets Act ("DTSA") will improve trade secret protection, which will incentivize innovation and benefit companies–large and small–in all industry sectors. I have seen the letter in support of this legislation signed by the Chamber of Commerce, the National Association of Manufacturers, tech associations, and an array of well-known companies in a variety of industries. But I can also tell you from my experience representing small businesses that they rely on trade secret law far more than patenting to protect their intellectual property, and this legislation will improve their ability to compete.

I applaud the work that Senators Hatch, Coons, Flake, Durbin, Tillis, Blumenthal, Klobuchar, Sessions, and Purdue have done on this legislation. The DTSA will create a unified, federal civil remedy, similar to what exists for other forms of intellectual property. It maintains the important balance between trade secret

---

[7] 18 U.S. C. §§ 1831-1839.

[8] See Pooley, Lemley and Toren, *Understanding the Economic Espionage Act of 1966*, 5 TEX. INT. PROP. L.J. 177, 205, 219 (1997)

owner and alleged misappropriator that exists under state law. And it adds an important, but limited, ability to seize a trade secret that has been stolen before the thief can take it out of the jurisdiction.

The approach of the DTSA is straightforward. It uses existing language of the EEA where appropriate, such as the definition of a trade secret, and where other language is required to define the civil aspects, such as misappropriation and damages, it uses language taken from the UTSA. Indeed, the only meaningful departure from the UTSA is to add a section allowing ex parte seizures of the misappropriated property. But even that portion draws from established provisions of the Lanham Act, tightened up considerably in order to discourage abuse.

The DTSA has received strong support from industry, but has been opposed by a group of law professors who published an "open letter" in 2014 criticizing the previous draft legislation,[9] and who have recently released another letter describing their concerns.[10] Mainly, they argue that we don't need federal legislation because state laws are uniform enough; that the DTSA's seizure provisions are too broad; and that the legislation would burden small companies with higher costs and interfere with the right of individuals to change jobs.

I strongly disagree with these arguments, which either ignore important facts or make implausible assumptions. As we have seen, the need for this legislation is clear; today's technologies and international markets pose threats that cannot adequately be addressed with inefficient state laws designed for a simpler and less risky time. And based on my experience in litigating similar cases, the ex parte seizure process is so narrow as to effectively eliminate the risk of abuse; the cost of trade secret litigation is not substantially different in federal court than it is in state court; and the DTSA will not be used to stop employees from changing jobs.

I will briefly explain each of these points here; a more detailed response to the arguments of the law professors' letters and published articles can be found in my article "*The Myth of the Trade Secret Troll: Why We Need a Federal Civil Claim for Trade Secret Misappropriation*," available at http://cpip.gmu.edu/wp-content/uploads/2015/11/James-Pooley-THE-MYTH-OF-THE-TRADE-SECRET-TROLL.pdf. A copy of the article is also attached to this statement.

---

9 http://cyberlaw.stanford.edu/files/blogs/FINAL%20Professors'%20Letter%20Opposing%20Trade%20Secret%20Legislation.pdf.

10 https://cyberlaw.stanford.edu/blog/2015/11/newprofessors-letter-opposing-defend-trade-secrets-act-2015.

The DTSA Will Create More Uniformity, Not "Undermine" It

The law professors argue not only that the DTSA is not necessary because the UTSA provides a harmonized legal environment, but also that the DTSA will "undermine" the uniformity that has already been achieved. The most obvious flaw in this argument is that the UTSA has not delivered the uniformity that its drafters had planned, and the state-by-state variations today are in some cases worse than had existed before the UTSA was proposed. This inconsistency creates a substantial burden for companies – including small businesses – that operate across state lines and who increasingly rely on trade secrets to protect their competitive advantage.

The professors point to the five-year statute of limitations in the DTSA as an example of undermining uniformity. But existing state versions of the UTSA already vary in their limitations periods from three to six years. They also claim that the EEA's definition of a "trade secret" is "broader" than the UTSA's, but this doesn't hold up to analysis. Both the EEA and the UTSA define a trade secret very broadly, but use different examples for illustration.[11] That one definition has more or different examples than the other doesn't matter, since the examples provided by each statute fit equally well under the definition of the other one. Finally, while the DTSA is not preemptive and would allow litigants a choice to sue in state or federal court, the professors fail to explain why having that choice should be deemed undesirable "forum-shopping," any more so than in other areas, such as trademark and securities law, where concurrent state and federal jurisdiction has long existed.

The Ex Parte Seizure Provisions Are Narrowly Tailored and Difficult To Abuse

In their most recent letter the law professors admit that the current language on ex parte seizure is "more limited in scope" than in the 2014 legislation. For example, only property "necessary to prevent the propagation or dissemination of the trade secret" can be seized, and the court must take possession of the property. These changes were made to a process that was already narrowly drawn to meet the need but go no farther. For an application to succeed, it must "clearly appear" to the court from "specific facts" sworn under oath that a

---

[11] The EEA, at 18 U.S.C. § 1839(3), describes the scope of "trade secret" as "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, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing." The shorter definition of UTSA § 1(4) is "information, including a formula, pattern, compilation, program device, method, technique, or process . . . ."

restraining order under Federal Rule 65(b) would be insufficient, and the court must make specific findings supporting a balance of harm in favor of the applicant due to an imminent danger of irreparable harm. The order must be written in a way that minimizes interruption to the defendant's related business and avoids any disruption to unrelated business. A hearing must be held within seven days, and during that time the defendant may apply to dissolve or modify the order.

As any lawyer who has practiced in this area can confirm, getting an ex parte order under these restrictions will be extremely difficult. And the consequences of getting it wrong will be severe: in addition to the usual sanctions that federal judges readily impose on parties and on lawyers when they feel they've been misled, the exposure to damages for wrongful seizure are not limited by the amount of the required bond. As a result, only the most seriously aggrieved plaintiff whose trade secrets are in imminent danger will take the risk of applying for an ex parte seizure.

The law professors argue that even this extraordinarily narrow remedy will still cause harm because all the defendant's computers and storage media might be seized, and because the defendant will be unable to immediately challenge the plaintiff's claim. But the first argument ignores the language of the DTSA that limits seizure to that property "necessary to prevent the propagation or dissemination" of the trade secret. The second argument also ignores the bill's clear statement that anyone "may move the court at any time to dissolve or modify the order." In my experience with ex parte restraining orders in trade secret cases, any defendant that can show there's been some terrible mistake will bring this to the court's attention promptly, sometimes the same day, and judges who realize that the plaintiff has misinformed them will have no hesitation in dissolving the order immediately.

In cases where a trade secret has been misappropriated and is in clear danger of being destroyed or transferred out of the jurisdiction, companies – including small businesses that rely heavily or exclusively on this kind of intellectual property – need the ability to get protection from a court without giving advance notice to the person who stole it. Of course, such an extraordinary proceeding should be strictly limited to minimize the risks of abuse. Under the DTSA, it is. The legislation achieves this balance by making a seizure very difficult and risky to get, while preventing collateral damage to the maximum extent possible.

Litigation Costs Will Not Be Higher, and May Be Lower, In Federal Court

The recent professors' letter asserts that the DTSA will "increase the length and cost of trade secret litigation." They base this argument only on the threshold requirement that the trade secret be "related to a product or service used in, or intended for use in, interstate or foreign commerce." But experience with other similar jurisdictional standards in federal statutes does not support the fear that

discovery or motion practice will be required on this issue. In almost all cases, the fact that the plaintiff's business meets the interstate commerce test will be obvious, the allegation will not be challenged at all, and there will be no impact on the cost or length of the litigation.

The second reason the professors give for their prediction of increased costs is that trade secret litigation is expensive, and the "liberal discovery standards" in federal court are likely to make litigation there more expensive. But federal courts have been handling trade secret cases for decades, under diversity or supplemental jurisdiction, and there is no evidence that costs there are any higher than they are to litigate in state courts. Most states' discovery standards are not materially different in any way that would affect trade secret litigation; and for the ones that do not employ standards as broad as federal courts, in my experience this can actually increase the cost of litigating in those states, as plaintiffs have to return repeatedly to court to get the evidence that they need to prove their case. Finally, beginning next month the revised Federal Rules of Civil Procedure will place a new emphasis on "proportionality" in discovery disputes,[12] and we have no reason to think that federal judges will apply that principle with any reduced rigor in trade secret cases.

The DTSA Ensures Free Mobility Of Labor

Finally, the professors speculate that certain language in the DTSA might be read to embrace the so-called "inevitable disclosure doctrine," which it claims "typically" leads a court to stop a departing employee from taking a new job. In fact, the "doctrine" is simply a label affixed by some commentators to a selection of court decisions applying the common-sense UTSA provision that "actual or threatened misappropriation may be enjoined." The vast majority of courts do not dwell on the "inevitable disclosure" label, but directly apply the statutory language about "threatened" misappropriation by thoughtfully considering the circumstantial evidence in individual cases. And where a court grants relief against threatened misappropriation, the result is only rarely to entirely block taking a new job.[13]

---

[12] Fed.R.Civ.Pro. 26.

[13] See Pooley, Trade Secrets §7.02[2] (Law Journal Press, updated 2014).

In any event, the DTSA does not imply either acceptance or rejection of the "doctrine." Significantly, it uses precisely the same "actual or threatened misappropriation" language as the UTSA. But – and this should have satisfied the professors' concerns – it adds a proviso that limits judicial discretion by prohibiting any injunction that would "prevent a person from accepting an offer of employment under conditions that avoid actual or threatened misappropriation." This provides additional assurance that a court will not interfere with any job offer unless it finds evidence that demonstrates actual or threatened misappropriation. And it is fully consistent with the law in every state that has enacted the UTSA, including California.

Conclusion

The DTSA is sorely needed to fill a gap in remedies available to U.S. businesses that now operate in an information-based, globalized economy. This is one of those special circumstances where parallel federal structures are required to address a critical set of interstate and international problems. The DTSA has been carefully fashioned to deter and punish abuse. Using well-established definitions and norms, it provides businesses a choice to file a familiar claim in an effective forum. And it accomplishes this without creating any new risks for small companies or individuals.

EXHIBIT 1

Forthcoming 23 George Mason L. Rev. __ (2016)

THE MYTH OF THE TRADE SECRET TROLL
Why We Need a Federal Civil Claim for Trade Secret Misappropriation

By James Pooley[1]

INTRODUCTION

Trade secret theft has been a federal crime since 1996, covered by the Economic Espionage Act ("EEA").[2] But civil misappropriation claims remain limited to state court filings under common law or local variants of the Uniform Trade Secrets Act ("UTSA"). Calls for federal jurisdiction have grown 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 have 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 was not acted on before Congress adjourned. A revised version is pending now, the Defend Trade Secrets Act of 2015 ("DTSA"), reflected in identical House (H.R.3326)[3] and Senate (S.1890)[4] bills.

---

[1] 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. He is also a co-author of the *Patent Case Management Judicial Guide* (Federal Judicial Center 2009, 2015). His most recent business book is *Secrets: Managing Information Assets in the Age of Cyberespionage* (Verus Press 2015). Mr. Pooley currently serves as Chairman of the Board of the National Inventors Hall of Fame, and is a past president of the American Intellectual Property Law Association. 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.

[2] 18 U.S. C. §§ 1831-1839.

[3] https://www.congress.gov/bill/114th-congress/house-bill/3326

[4] https://www.congress.gov/bill/114th-congress/senate-bill/1890

The current draft legislation has received broad support from a variety of industries,[5] and also enjoys unusually bipartisan political sponsorship.[6] 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.[7] Among other objections, they complained that the seizure provisions created inappropriate risks to third parties, that injunctions were not sufficiently limited, and that increasing available remedies for misappropriation would lead to decreased employee mobility.

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.[8] In the most recent of these, a new argument was offered: that federalizing civil trade secret law would unleash a dangerous new class of litigants called "trade secret trolls," who, like their patent counterparts, would terrorize the community of legitimate innovators.

On July 29, 2015, the current legislation was introduced simultaneously in the House and Senate.[9] 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. On August 3, the 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."[10] On November 17th, those authors were joined by 29 others in another open letter, contending that the legislation

---

[5] See http://www.hatch.senate.gov/public/_cache/files/09ce963b-6166-4156-b924-ab1c7f4098f5/DTSA%20Senate%20Support%20Letter.pdf.

[6] As of November 4, 2015, H.R.3326 had 65 cosponsors, 45 Republican and 20 Democrat, and S.1890 had ten cosponsors, six Republican and four Democrat. See https://www.congress.gov/bill/114th-congress/house-bill/3326/cosponsors, and https://www.congress.gov/bill/114th-congress/senate-bill/1890/cosponsors.

[7] *Professors' Letter in Opposition to the "Defend Trade Secrets Act of 2014" (S. 2267) and the "Trade Secrets Protection Act of 2014" (H.R. 5233)*, August 26, 2014, available at http://cyberlaw.stanford.edu/files/blogs/FINAL%20Professors'%20Letter%20Opposing%20Trade%20Secret%20Legislation.pdf.

[8] Zoe Argento, *Killing the Golden Goose: The Dangers of Strengthening Domestic Trade Secret Rights In Response to Cyber-Misappropriation*, 16 YALE J.L. & TECH. 172 (2014); Christopher B. Seaman, *The Case Against Federalizing Trade Secrecy*, 101 VA. L.R. 317 (2015); David S. Levine and Sharon K. Sandeen, *Here Come the Trade Secret Trolls*, 71 WASH. & LEE L.R. ONLINE 230 (2015).

[9] http://dougcollins.house.gov/press-releases/defend-trade-secrets-act-introduced-in-house-and-senate/

[10] David S. Levine and Sharon K. Sandeen, *Open Letter to the Sponsors of the Revised Defend Trade Secrets Act*, (2015), available at http://cyberlaw.stanford.edu/publications/open-letter-sponsors-revised-defend-trade-secrets-act. 2015).

would harm small business, unduly restrict labor mobility, increase the cost of litigation and de-harmonize trade secret law.[11]

In this article I offer 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 I will explain in more detail below, federalizing civil trade secret law would fill 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 bills would accomplish 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 would risk invoking the procedure. Having no pre-emptive effect, the federal law would leave in place all relevant state laws and policies, including those relating to mobility of labor. Finally, I will argue 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.

BACKGROUND: 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). The law's principles emerged from the results and reasoning of individual cases enforcing promises of confidentiality. 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.[12] But the courts' logical emphasis on protecting a confidential relationship led the original framers of the Restatement to categorize trade secrets within the law of torts. The 1939 Restatement (First) of Torts §§ 757-59 thus was the first step in "harmonizing" state common law. However, forty years later when the Second Restatement 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

---

[11] *Professors' Letter in Opposition to the Defend Trade Secrets Act of 2015 (S. 1890, H.R. 3326)*, November 17, 2015, available at https://cyberlaw.stanford.edu/blog/2015/11/new-professors-letter-opposing-defend-trade-secrets-act-2015.

[12] See, for example, Peabody v. Norfolk, 98 Mass. 452, 458 (Mass. 1868): If one "invents or discovers, and keeps secret, a process of manufacture, . . . he 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 it should not – has long been debated, but since secret information can be transferred and taxed like other property, the question seems to be moot. See JAMES H. POOLEY, TRADE SECRETS §1.02[8] (Law Journal Press, updated 2014).

tort law could no longer provide the central rationale, and it was left to a future restatement to address the issue.[13]

This explanation was published about five years after the most important development in trade secret law of the twentieth century: the opinion of the U.S. Supreme Court in *Kewanee Oil Co. v. Bicron Corp.*,[14] in which petitioners claimed that state trade secret law should be pre-empted as conflicting with federal patent law, because the latter requires disclosure and the former protects against it. Finding no pre-emption, the 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."[15] 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.[16] 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.[17]

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 Uniform Trade Secrets Act.[18] 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.[19] Of course, the lack of treatment by the Restatement (Second) reinforced the need for an alternative path toward uniformity.

---

[13] RESTATEMENT (SECOND) OF TORTS 1-2 (1979) Div. 9, Introductory Note: "the 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."

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

[15] *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." 416 U.S. at 487.

[16] *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 416 U.S. at 493: "Trade secret law promotes the sharing of knowledge, and the efficient operation of industry . . . ."

[17] *Id.* at 489-90 ("Where patent law acts as a barrier, trade secret law functions relatively as a sieve.")

[18] Unif. Trade Secrets Act Refs and Annos, available at http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf.

[19] *Ibid.*

The UTSA tried to codify the fundamental principles of the existing common law of trade secrets, "preserving its essential distinction from patent law."[20] 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." Section 757 of the Restatement had required that secrets be "in continuous use" in a business. Now, "ephemeral" data (such as private bids) and "negative" secrets (such as the results of failed experiments) would be protectable. On the other hand, under the Restatement (First) the trade secret owner's self-help measures had been only a factor for consideration; under the UTSA those "reasonable efforts" became part of the required proof to establish a protectable secret.

What could constitute a misappropriation was also changed. Under the original Restatement mere acquisition of a secret, even if improper, was not actionable absent proof of use or further disclosure; while the UTSA addressed acquisition where the actor had reason to know that it had been accomplished by improper means.[21] In the same vein, the Restatement of Torts had provided "immunity" for third parties who received secret information in good faith; 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.[22]

But as its name suggests, a primary objective of the UTSA was uniformity. 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.[23] And quite a few states have enacted a customized version of the official one.[24] The notes to the Uniform Act 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

---

[20] *Ibid.*

[21] UTSA §1(2). See also RESTATEMENT (THIRD) OF UNFAIR COMPETITION §40, cmt. b (1995): "The prior 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."

[22] UTSA §2(b). See comments.

[23] See Linda B. Samuels and Bryan K. Johnson, *The Uniform Trade Secrets Act: The States' Response*, 24 CREIGHTON L. REV. 49, 51-53 (1990).

[24] See Sid Leach, *Anything but Uniform: A State-By-State Comparison of the Key Differences in the Uniform Trade Secrets Act* (2015) available at 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

indicated by statutory notes."[25] In other words, the variations are too numerous to mention.

Academics and practitioners have noted this lack of uniformity of the UTSA.[26] A few examples will help illustrate the scope of the problem. California dropped the language requiring that a trade secret be not "readily ascertainable," with the result that the defendant is required to specially plead that circumstance as an affirmative defense.[27] Illinois also eliminated the "readily ascertainable" language, and it prohibits royalty injunction orders, sets a different limitations period and allows permanent injunctions.[28] Idaho requires that computer programs carry a "copyright or other proprietary or confidential marking" to qualify for protection.[29] Georgia limits protection of customer lists to physical embodiments, in effect allowing employees to appropriate such information in (human) memory.[30] 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.[31]

In 1995 the Restatement (Third) of Unfair Competition was released, including a new treatment of the law of trade secrets at §§39-45. 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 of Torts, sometimes applying its (now minority) position on, for example, the need to show "continuous use" of secret information.[32]

---

[25] See UTSA, note 18 supra. The annotations list sixteen state variation for §1 of the Act (definitions), seventeen for §2 (injunctive relief), seventeen for §3 (damages), seven for §4 (attorney's fees), one for §5 (preservation of secrecy), four for §6 (limitations), and eighteen for §7 (effect on other laws). Only the title and the sections on severability and (ironically) uniformity have escaped modification by state legislatures.

[26] See, e.g., Marina Lao, *Federalizing Trade Secrets Law in an Information Economy*, 59 OHIO ST. L.J. 1633, 1661-65 (1999); Christopher Rebel J. Pace, *The Case for a Federal Trade Secrets Act*, 8 HARV. J.L. & TECH. 427, 442-44; David S. Almeling, *Four Reasons to Enact a Federal Trade Secrets Act*, 19 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 769, 773-74.

[27] See James H. Pooley, *The Uniform Trade Secrets Act: California Civil Code 3426*, 1 SANTA CLARA H.T. L. J 193, 197-98 (1985).

[28] 765 ILCS §1065 (1988).

[29] Idaho Code §48-801(4)(c).

[30] See Tronitec, Inc. v Shealy, 249 Ga.App. 442, 547 S.E.2d 749, 754 (Ga.App. 2001).

[31] For an accessible comparison of South Carolina's current statute with its prior (and more conventional) version of the UTSA, see 2 Brian M. Malsberger, TRADE SECRETS: A STATE-BY-STATE SURVEY (5th ed. 2015).

[32] See, e.g., Mann v. The Cooper Tire Co., 33 A.D.3d 24, 32, 816 N.Y.S.2d 45, 53 (N.Y. App. Div. 2006) (applying "continuous use" requirement to deny trade secret protection to formula for

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 signed into law.[33] The process of legislative consideration was swift and bumpy, with some last-minute amendments.[34] 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.[35] 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,[36] 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.[37]

PROPOSED LEGISLATION TO ADD A CIVIL CLAIM TO EEA

Calls for a federal trade secret law with a private right of action had already begun before the EEA was passed.[38] After it became law, scholars noted the anomaly and suggested that, because the national economy had become primarily knowledge-based, because even with the UTSA state law was not uniform, and to bring the U.S. unquestionably into compliance with its obligations under the TRIPS Agreement,[39] a broad federal law should be enacted.[40] More recent commentary, while continuing to emphasize the drawbacks of variations in state law, also has pointed out the economic advantages of federalization, particularly for small businesses, which rely more heavily on secrecy than on patenting,[41]as

---

tire rubber), and Bear, Stearns Funding, Inc. v. Interface Group-Nevada, Inc., 361 F.Supp.2d 283, 305-306 (S.D.N.Y. 2005) (applying "ephemeral events" exception).

[33] See generally James H.A. Pooley, Mark A. Lemley and Peter J. Toren, *Understanding the Economic Espionage Act of 1966*, 5 TEX. INT. PROP. L.J. 177 (1997)

[34] *Id.* at 187.

[35] Peter J. Toren, *An Economic Analysis of Economic Espionage Prosecutions: What Companies Can Learn From It and What the Government Should Be Doing About It!*, 84 BNA PATENT, TRADEMARK & COPYRIGHT J. 884, 2-3 (2012).

[36] See Pooley, Lemley and Toren, note 32 supra, at 219.

[37] Id. at 205; Toren, supra note 35, at 3,

[38] See, for example, Pace, note 26 supra (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 U.S. was in full compliance with its obligations under international treaties).

[39] See https://www.wto.org/english/tratop_e/trips_e/t_agm3d_e.htm#7. Because the UTSA was used as the pattern for the international standard reflected in Article 39 of TRIPS, it is ironic that the U.S. has not established its own national standard but left civil enforcement exclusively in the hands of individual states. My experience as a diplomat dealing with intellectual property and trade issues suggests that eliminating this strange incongruity will strengthen the hand of U.S. trade negotiators.

[40] See, e.g., Lao, note 26 supra.

[41] See Almeling, note 26 supra.

well as the procedural advantages for trade secret owners, including national service of process.[42] 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 – would 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.[43]

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.[44] 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. That effort failed to secure a vote on the amendment. The following year Senator Coons, along with Sens. 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. 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 Sens. 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. Earlier, S.1770 had been introduced by Sen. Flake 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 anti-suit injunctions. In the House, Rep. 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 detailed constraints on the seizure process. Finally, Rep. Zoe Lofgren introduced H.R. 2466, the Private Right of Action Against Theft of Trade Secrets Act, a two-

---

[42] 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 has recently 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).

[43] See Seaman, note 8 supra, 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 current bills are explicitly non-preemptive and so the concern is even more abstract.

[44] S.A. 729 to S.1619, the Currency Exchange Rate Oversight Reform Act of 2011, available at https://www.congress.gov/amendment/112th-congress/senate-amendment/729/text?q=%7B%22search%22%3A%5B%22SAmdt+729%22%5D%7D&resultIndex=2727.

paragraph amendment to the EEA that would have added a civil cause of action, but without the ex parte seizure provisions. 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.

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."[45] 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. 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. 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. Requiring definition of secrets early in litigation to address jurisdiction issues, it added, could increase the risk of improper disclosure. 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." 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."

The professors' letter was followed months later by several published articles that correctly anticipated continuing efforts in Congress to federalize trade secret law. I will provide a brief summary and critique of those articles below, as a prelude to a more thorough discussion of why I believe the current legislation should be enacted, but at this point I will respond briefly to the arguments raised in the 2014 letter and then to those raised recently in the letter of November 17, 2015.

While reasonable people can differ over how much variation in state statutes can be accepted while still calling them "uniform," it should be apparent from the examples provided in the background section of this paper that the UTSA cannot fairly be deemed "uniform" without serious caveats. But in the 2014 letter, we see no acknowledgement of the substantial variation that exists, and that can bedevil companies with operations in multiple states. Cross-border procedural hurdles are

[45] See *2014 Professors' Letter*, note 7 supra.

not made to disappear by the "rich body of law" that informs how to deal with them.[46] And diversity jurisdiction must rest on complete diversity of citizenship, which does not exist in the common trade secret case that involves one or more local actors.

Although a non-preemptive 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. They have also proven capable of using protective orders to prevent loss of secrecy in the courtroom. 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.

I acknowledge the professors' initial concerns over the ex parte seizure provisions, protecting the right to reverse engineer, and appropriate limitations on injunctions. But as it should become clear in the discussion that follows, those concerns have been adequately addressed by the current legislation.

It is on their last cluster of arguments that I find myself in strongest disagreement with the professors' 2014 letter. 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. As the Supreme Court explained in *Kewanee*: "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."[47]

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 legislation would affect 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 would not be changed at all.

The concern over mobility of labor is misplaced for similar reasons. If the worry is about enforcement of noncompete covenants, the answer is that the bills, having no pre-emptive effect, would not impact state law or policy in that area. And as we will see, anxiety over application of the "inevitable disclosure doctrine" is overdone.

---

[46] *Id.* at 3

[47] See *Kewanee*, note 14 supra, at 486.

The 2015 professors' letter makes several new or revised arguments, none of which withstands scrutiny. First, while admitting that the current language on ex parte seizure is "more limited in scope" than the 2014 legislation (for example, only property "necessary to prevent the propagation or dissemination of the trade secret" can be seized), the professors think this tightening is not enough and that the provision "may still result in significant harm." The letter provides no evidence for this,[48] but speculates 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." As I will explain below, these abstract fears are ungrounded and exaggerated.

Second, the letter asserts that new language, added to ensure that mobility of labor is respected, embraces the so-called "inevitable disclosure doctrine," which is nothing more than a method of analysis under the UTSA provision for injunctions against "threatened misappropriation." Although this method has been applied in a majority of jurisdictions, resulting in a wide range of remedies falling far short of prohibiting competitive employment, the professors' argument is based on the false premise that it amounts to a judge-made noncompetition agreement.[49] I will explain below in more detail why this is a straw man argument.

Third, the professors claim that the DTSA "likely will increase the length and cost of trade secret litigation," with consequential damage to "small businesses and startups." As with many of their other points of opposition, this one rests on overstatement and speculation. Although the law would only apply 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

---

[48] The letter relies 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 (October 30, 2015), available at http://www.corpcounsel.com/id=1202741205249/The-Defend-Trade-Secrets-Act-Is-Strong-Medicine-Is-It-Too-Strong?slreturn=20151009142017. The author incorrectly asserts that the DTSA would allow a court to "shut down the defendant's business for up to a week." His fears of "trade secret trolling" are 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." But he fails 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.

[49] The letter claims, 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." See *2015 Professors' Letter*, note 11 supra, at 4-5. My own 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." See Pooley, *Trade Secrets*, note 12 supra, at §7.02[2]. Indeed, 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. *Ibid.*

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. And although the letter cites 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.[50]

Finally, the letter returns 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." As I have already 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. Indeed, one might suppose that is why the DTSA enjoys such broad support in the business community. The professors also submit, without offering analysis or examples, that whatever uniformity now exists will be undermined by the EEA's supposedly "broader" definition of a trade secret.[51] Finally, they point 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."

I turn now to the law review articles that followed issuance of the 2014 professors' letter. The first of these, by Zoe Argento of Roger Williams University Law School, is entitled *Killing the Golden Goose: the Dangers of Strengthening Domestic Trade Secret Rights in Response to Cyber-Misappropriation.*[52] 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. From there she proceeds to critique the legislation mainly on the basis that it would not solve that problem. 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 bills confront. Instead, their main objective is to make it more practical for trade secret owners, in an age where their rights

[50] Indeed, there is reason to believe that federal courts, applying the newly reinforced requirement of "proportionality" in the Federal Rules of Civil Procedure, will exercise their authority to rein in wasteful discovery practices.

[51] 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) 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." UTSA §1(4).

[52] See Argento, note 8 supra.

can be electronically compromised in mere seconds, to secure effective judicial relief.

While I disagree with some of the other propositions advanced in the Argento article, in particular her treatment of the "property" theory,[53] it is helpful to point out a few illuminating statements. First she acknowledges that the North Carolina and Alabama trade secret statutes "vary significantly" from the UTSA.[54] 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.[55]

The second major article to appear in opposition to the proposed legislation is by Christopher Seaman of Washington and Lee University School of Law, titled *The Case Against Federalizing Trade Secrecy*.[56] 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 bills, 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.[57] And while one of his key theses is that federalization risks abandoning the advantage of the states as

---

[53] *Id.* at 182-86, where the author equates 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. I believe that the dispute between the "property" and "confidence" schools of thought is of historical interest only, and that modern law recognizes both interests. See note11 supra and accompanying text. I also am concerned with Professor Argento's choice of vague and undefined terms in relation to trade secret law, such as "over-protection," "over-broad" and "strong" protection. In my experience, this kind of value-freighted terminology is too frequently used in place of rigorous analysis of the competing interests that are almost always present in this area of the law.

[54] *Id.* at 178 n. 23. See also p. 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."

[55] *Id.* at 210.

[56] See Seaman, note 8 supra.

[57] For example, he 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. He is probably correct that "most" of the 47 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. See note 25 supra and accompanying text. 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

"laboratories" for experimentation with differing policies,[58] 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.

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 public. In fact, he hypothesizes a "bell curve" in which "weak" protection of secrets will (as *Kewanee* recognized) lead to less disclosure, but in which "too much trade secret protection" will have the same result.[59] 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 pending bills. Just what is "too strong" in this context?[60] The way he uses the phrase, the substantive (scope of rights) is conflated with the procedural (choice of court where rights will be enforced). If one considers the shift in trade secret law from the 1939 Restatement of Torts to the modern rule of the UTSA, there was undoubtedly some "strengthening" taking place. 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."[61] 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.[62]

---

[58] *Id.* at 365.

[59] *Id.* at 385.

[60] The "strength" abstraction runs out of control when Professor Seaman speculates that if Congress passes the Defend Trade Secrets Act, later it "may enact additional changes that further strengthen the rights of trade secret owners." *Id.* at 382.

[61] *Id* at 380.

[62] See Pooley, *Trade Secrets*, note 12 supra, at §10.07[4]. *Cf. TianRui Group. Co. Ltd. v. Int'l Trade Com'n*, 661 F.3d 1322, 1343 (Fed. Cir. 2011) (Moore, J., dissenting). In reaction to the notion of extraterritorial application of U.S. trade secret law to a misappropriation occurring entirely in a foreign country, Judge Moore complained that the result would provide "an additional incentive to inventors to keep their innovation secret," which she felt would in turn "den[y] society the benefits of disclosure stemming from the patent system, which are anathema to trade secrets." While I agree that robust domestic remedies for foreign theft of secrets belonging to U.S. companies can provide some additional encouragement to rely on secrecy, I see that as fully consistent with the Supreme Court's holding in *Kewanee* that trade secret law is complementary to the patent system. After all, the policy goal of the patent law is not disclosure itself but encouragement of invention, and that is also a primary policy behind trade secret law. *Kewanee*, note 14 supra, at 493.

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."[63] But he argues that these benefits can be achieved without amending the EEA, by litigants asserting their rights to federal diversity and supplemental jurisdiction.[64] Of course, 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.[65] Indeed, the weakness of his argument is underscored by his proposed alternative to the bills: Congress should remove the complete diversity requirement just for trade secret cases.[66]

The most unusual of the three articles is *Here Come the Trade Secret Trolls*, by David Levine of Elon University School of Law and Sharon Sandeen of Hamline University School of Law.[67] It relies heavily on the Argento[68] and Seaman articles but does not supply any new evidence or fresh analysis.[69] Instead, its main contribution is to repeat in various ways a strikingly implausible prediction: that the pending legislation 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."[70]

---

[63] See Seaman, note 8 supra, at 368.

[64] *Id.* at 369.

[65] See 28 U.S. C. §1367; United Mine Workers of America v. Gibbs, 383 U.S. 715, 725 (1966); Tech Enterprises, 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).

[66] See Seaman, note 8 supra, at 386.

[67] See *Trolls*, note 8 supra.

[68] Like Argento, the authors of *Trolls* begin their attack on the bills by assuming incorrectly that the only issue being addressed is cyberhacking. For this assumption they rely on a press release from Sen. 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." 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 (at 238-43) that we need more data on cyberhacking before considering legislation.

[69] 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 citation of any reference, that existing laws addressing interstate discovery "are not onerous" and that trade secret lawsuits involving foreign defendants are "rare." *Id.* at 251.

[70] *Id* at 252.

"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. Trade secrets, in stark contrast, are private rights that can be asserted only against a thief or one who has breached a confidence. Although frivolous trade secret lawsuits have occasionally been filed, existing law has sufficient sanctions to deal with those instances, and the bills contain precisely the same penalties. As I will explain 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 pending legislation will cause this imagined beast to materialize.

THE 2015 BILLS

The DTSA is reflected in identical bills filed in the Senate (S. 1890) and House (H.R. 3326) on July 29, 2015. For the most part, the legislation would amend §1836 of the EEA, to provide a civil cause of action for any "person aggrieved by misappropriation of a trade secret" related to interstate commerce, adding sections on civil seizure and on remedies for misappropriation.

The provisions covering ex parte seizure of property are extensive and tightly drawn. An application must be accompanied by a sworn affidavit from which it "clearly" appears "from specific facts" that injunctive orders under FRCP Rule 65 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. The application must also demonstrate likelihood of prevailing on the elements of the misappropriation claim, describe with particularity the material to be seized, prove the danger that the material will be moved or lost, and certify that there has been no publicity of the requested seizure.[71]

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 directly related business and preventing interruption of the defendant's unrelated operations. The plaintiff must post a bond to secure liability for a seizure that turns out not to have been justified, but the amount of the bond will not limit damages that can be claimed for wrongful seizure. The order (which must be served by federal marshals) can remain in effect only seven days before a hearing

[71] The Defend Trade Secrets Act of 2015, S. 1890, 114th Cong. §§2(b)(2)(A)(ii)(IV-VII) (2015), see notes 3 & 4 supra.

is held, at which the plaintiff must show facts justifying continuation of the order and at which the court may modify the normal discovery timeframes.[72] (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.)

Following execution of the seizure order, the defendant or anyone else affected can move at any time to dissolve or modify it. The seized property must be held by the court, and electronic files will be kept unconnected with any network, including the Internet. Access must be controlled, and no copies may be made. On motion the court may order any electronic files to be encrypted.

Regarding the more prosaic aspects of trade secret remedies, the bills follow closely the language of the Uniform Trade Secrets Act, allowing for injunctions against "actual or threatened" misappropriation, but adding a limitation that any order may "not prevent a person from accepting an offer of employment under conditions that avoid actual or threatened misappropriation."[73] This provision was apparently intended to address concerns about employee mobility and the "inevitable disclosure doctrine," a subject that was raised in the professors' letters and is discussed in more detail below. 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.[74]

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. Willful and malicious misappropriation can trigger an award of treble damages, plus attorney's fees. Consistent with the UTSA, attorney's fees may also be awarded to a defendant if a claim of misappropriation is found to have been prosecuted in bad faith.[75]

The bills set a limitations period of five years, which is longer than the three-year period in the UTSA, but within the range of limitation periods actually established by state legislatures.[76] Significantly, given the EEA's special provisions defining

---

[72] *Id.* at §§2(b)(2)(B-D).

[73] *Id.* at §2(b)(3)(A)(i).

[74] *Id.* at §2(b)(3)(A)(iii).

[75] *Id.* at §2(b)(3)(B-D).

[76] Although most states have adopted the three-year period proposed by the UTSA, in Maine it is four years. Illinois, Missouri and Georgia designate five years. And Vermont allows six years. Apart from coherence with other state law-based causes of action, a legislature's choice of time is essentially arbitrary in balancing the plaintiff's need to discover and build its case with the general risk of fading memories and lost evidence. However, there are good reasons to be generous in allowing time for the plaintiff to sue, particularly where, as here, the "continuing tort" theory is not available, and the trade secret owner will be judged in hindsight about whether it exercised

criminal behavior, the bills add 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 2014 professors' letter.[77]

The legislation is expressly non-preemptive, leaving the states free to continue to fashion and enforce their own laws relative to trade secrets.[78] It adds a requirement for a biennial report from the Attorney General, working with the IP Enforcement Coordinator and the Director of the PTO, on trade secret theft, describing enforcement in foreign jurisdictions, actions taken by U.S. agencies, and recommendations.[79] Finally, the bills include a statement of the "sense of Congress" that trade secret theft is an international problem that harms both companies and their employees.[80]

At last count, H.R. 3326 has 65 cosponsors, comprising 45 Republicans and 20 Democrats. The Senate bill has ten cosponsors, of whom six are Republicans and four are Democrats. It hardly needs emphasis that such bipartisan support for legislation is uncommon. Industry has also expressed strong support.[81]

THE PROPOSED LEGISLATION MEETS A REAL NEED

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 state's 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

---

"reasonable diligence" to discover the first act of misappropriation. See Pooley, *Trade Secrets*, note 12 supra, at §10.09[2].

[77] The Defend Trade Secrets Act of 2015, S. 1890, 114th Cong. §2(b)Definitions(6)(B) (2015), see notes 3 & 4 supra.

[78] *Id.* at §2(f).

[79] *Id.* at §3(b).

[80] *Id.* at §4.

[81] See "Senators Hatch, Coons Urge Passage of Trade Secrets Bill," available at http://www.hatch.senate.gov/public/index.cfm/2015/10/senators-hatch-coons-urge-passage-of-trade-secrets-bill. (press release detailing supporting organizations)

profile of holding trade secrets has been profoundly and irretrievably altered. Never have information assets been so 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% in 1975 to 68% in 1995 to 84% today.[82] 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-Mellon,[83] and was confirmed by a 2012 report from the National Science Foundation and the Census Bureau. 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.[84]

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. 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 pending legislation, 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 be a match for the risk. Viewed in that light, the current situation faced by U.S. industry is sadly inadequate. State laws are far from uniform, placing a burden on companies with regional or national operations.[85] This is not an abstract problem. A trade secret owner who learns of

---

[82] *Ocean Tomo Releases 2015 Annual Study of Intangible Asset Market Value*, (March 5, 2015), http://www.oceantomo.com/blog/2015/03-05-ocean-tomo-2015-intangible-asset-market-value/

[83] Wesley M. Cohen, et al., *Protecting Their Intellectual Assets: Appropriability Conditions and Why U.S. Manufacturing Firms Patent (or Not)*, NBER Working Paper No. 7552 (2000), available at http://www.nber.org/papers/w7552.

[84] John E. Jankowski, *Business Use of Intellectual Property Protection Documented in NSF Survey*, NSF 12-307 (2012), available at http://www.nsf.gov/statistics/infbrief/nsf12307/

[85] 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

an impending misappropriation in a location remote from its headquarters may be faced with going to a county court, appearing before a motions judge sitting on a rotation system or operating under local rules and customs that may limit or even deny direct access to the judge. And if there is access, the judge is unlikely to be very familiar with complex issues of comity and personal jurisdiction that are common to international disputes, and may therefore be reluctant to act.

But even where the boundaries are only between states, the existing system is 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.[86]

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 current EEA criminal provisions.[87] The reality is starkly different, as described by former EEA prosecutor Peter Toren, who has analyzed the relatively "languid pace" of filings (eight per year on average) under the statute.[88] 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. This "reluctance to prosecute EEA cases is reinforced" by internal guidelines that disfavor prosecution when the victim has a civil remedy, as most do.

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 provides a

---

plaintiff is permitted until the plaintiff has described the relevant secrets at a level of detail ("reasonable particularity") that satisfies the court. Cal. Code Civ. Pro. §2019.210.

[86] See Halligan, *Revisited 2015*, note 42 supra, at 494.

[87] See *Trolls*, note 8 supra, at 249-50, 254.

[88] See Toren, note 35 supra.

satisfactory solution. Federal courts, however, can provide 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.[89] 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.[90]

Having reliable access to federal courts in trade secret cases requires that the EEA be amended. It is not sufficient to say that plaintiffs can get there through diversity jurisdiction, since complete diversity is required, and many trade secret cases will not qualify due to the involvement of one or more local defendants. And supplemental jurisdiction is not the answer either, since 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.[91]

THE SEIZURE REMEDY IS NARROWLY DRAWN TO A SPECIFIC NEED

As already discussed, modern digital technology has made trade secrets more vulnerable to loss. 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 the irreparable harm. The remedy of ex parte seizure is not unknown in federal cases dealing with trade secrets, since 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

---

[89] See Halligan, *Revisited 2015*, note 42 supra, at 493-94.

[90] See Greenberg v. Croydon Plastics Co., Inc., 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."

[91] See note 64 supra and accompanying text.

should not be required.[92] The DTSA preserves these conditions and goes well beyond Rule 65(b) in prescribing other conditions and restrictions, to ensure that orders are available only in the clearest and most compelling cases, and only to "prevent the propagation or dissemination of the trade secret."

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 engage in timely exit interviews."[93] Such self-help measures can work well in an environment where the departing employee is cooperative, but in a more hostile situation 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.[94] 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 . . . ."[95] 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, we also should insist that the remedy be drawn narrowly, to permit intervention only to the extent required, with appropriate disincentives against abuse. The bills appear to strike that balance well. In the first place they demand compelling proof of a real risk of disappearance or destruction of the trade secrets. 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." The plaintiff's abstract fear – for example, based on the defendant's access to the information and its easily transportable character – will not be enough.[96] 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.

---

[92] Cf. First Technology Safety Systems, 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).

[93] See *Trolls*, note 8 supra, at 253.

[94] *Ibid.*

[95] *Ibid.*

[96] See *First Technology Safety Systems, Inc.*, note 91 supra.

This statutory framework is not new; it has been used in the field of counterfeit goods.[97] The Lanham Act provisions for ex parte seizure are nearly identical to those in the bills, allowing the remedy only where it "clearly appears from specific facts" that another kind of order would not suffice.[98] 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.[99]

The bills' requirements for trade secret seizure are even more constrained than those in the Lanham Act. The order must minimize interruption to the defendant's related business, and avoid any disruption to unrelated businesses, to prevent collateral damage. And while the Lanham Act allows a hearing to be set from ten to fifteen days later, the bills impose a strict seven-day limit for holding a hearing. During that time the defendant is free to make an application to dissolve or modify the seizure order.[100] Special provisions are added to protect the integrity of information, by prohibiting copies, prohibiting connection to a network, restricting access, and allowing encryption.

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. Moreover, federal judges are not known for suffering fools gladly, and they have substantial powers to sanction inappropriate behavior under Rule 11.[101] 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 could exact a settlement payment by sending out letters threatening an ex parte seizure application.[102] But

---

[97] Internationally, the comparable "Anton Piller" seizure order has been regularly used in the United Kingdom and Canada. Anton Piller KG v. Manufacturing Processes Ltd & Ors [1975] EWCA Civ 12, [1976] 1 All ER 779 (8 Dec. 1975). Celanese Canada Inc. v. Murray Demolition Corp. 2006 SCC 36, [2006] 2 SCR 189 (27 July 2006).

[98] 15 U.S.C. §1116(d)(4)(B).

[99] 15 U.S.C. §1116(d)(5)-(7).

[100] It is therefore difficult to comprehend how the authors of the 2015 professors' 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 *2015 Professors' Letter*, note 11 supra, at 3. There is no reason that the defendant could not mount such a challenge the same day or the next.

[101] Fed. Rules Civ. Proc. Rule 11, 28 U.S.C.A.

[102] See *Trolls*, note 8 supra, at 255 (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

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.

THE BILLS DO NOT CHALLENGE STATE LAWS OR POLICIES ON MOBILITY OF LABOR

The professors' letter of August 2014 claimed that the previous draft legislation would "limit mobility of labor,"[103] but did not explain exactly why this was so. In the articles published since then, 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."[104] This was a novel reinterpretation of the rationale laid down by the Supreme Court in *Kewanee*, 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.[105] From her public interest-centered position, Argento argued that departing employees can serve society through a "cross-pollination effect" resulting from "seepage of useful information that benefits the public."[106]

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.[107] Using "inevitable disclosure" as an example, 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.[108] He forecast the result that "firms that engage in innovation protected by trade secrecy would no

---

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.").

[103] See *2014 Professors' Letter*, note 7 supra, at 6.

[104] See Argento, note 8 supra, at 202.

[105] See *Kewanee*, note 14 supra, at 485-86.

[106] See Argento, note 8 supra, at 188.

[107] Pepsico, Inc. v. Redmond, 54 F.3d 1262 (7th Cir. 1995).

[108] See Seaman, note 8 supra, at 365-66.

longer be free to choose whether to conduct their research in states that follow (or do not follow) the inevitable disclosure doctrine."[109]

The 2015 professors' letter goes 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."[110] The specific language in the bills begins with a provision taken directly from the UTSA, which as already noted authorizes injunctions to prevent "actual or threatened misappropriation."[111] The DTSA adds this proviso: "provided the order does not prevent a person from accepting an offer of employment under conditions that avoid actual or threatened misappropriation." The plain meaning reflects an intent that courts be able to set reasonable conditions on employment, in order to avoid circumstances that would threaten the integrity of secret information. But for the professors, the proviso triggers a focus on the assumed evil of the abstract "doctrine," an assumption that is unjustified.

Commentators who rail against the "inevitable disclosure doctrine" are conflating a court's mode of analysis with a particular result: an order preventing someone from taking a job. They use the coined label to conjure the image of a judicially-imposed post hoc noncompetition agreement. But the reality is nothing more than straightforward application of the UTSA's authorization of injunctions against "actual or threatened misappropriation." Giving force to this language means that courts may intervene not only where misappropriation already has happened, but also where it is likely to happen because it has been "threatened." And unless one takes the position that threats must always be verbal to be actionable, it follows that courts may issue injunctions when circumstantial evidence – including suspicious and dishonest behavior by a departing employee – strongly indicates that the trade secret holder's rights will be endangered by that person's immediate transfer to a direct competitor to do an identical job.

---

[109] *Id.* at 367. Professor Seaman's fears are not grounded in fact. First, the bills are not preemptive, leaving state legislatures and courts free to experiment on any issues that they deem important. And so 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.

[110] See *2015 Professors' Letter*, note 11 supra, 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." Quoting On Amir and Orly Lobel, *Driving Performance: A Growth Theory of Noncompete Law*, 16 STAN. TECH. L. REV. 833, 837-38 (2013). The authors of the 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. 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.

[111] See UTSA, note 18 supra, at §2.

This was the situation in *Pepsico*, where Redmond had been a general manager with access to all of Pepsico's latest strategic information regarding its sports drink products, and sought to take the equivalent position with a direct competitor at a critical time. Redmond had been untruthful when discussing his future plans with his employer, and this element of untrustworthiness was a major factor in the court's decision to block the move, although it did so only for five months.[112] Indeed, in actual application of the "inevitable disclosure doctrine" by courts, a flat prohibition against taking a job is rare; much more common is an order that places reasonable conditions, such as having to work in a different area of the company for a period of time, while the risk of inadvertent disclosure subsides and the time value of the information decreases.[113] Therefore, it is analytically inappropriate to sweep into one category the entire range of prophylactic measures that should be available to a court in the case of circumstantial threats to trade secrets. That is why the current language of the bills is responsive to the concern expressed in the original professors' letter: it removes the possibility of a blanket order prohibiting accepting a job offer but preserves the court's important discretion to control the "conditions" of such employment in order to avoid "actual or threatened misappropriation".[114] The claim that the DTSA would interfere with employee mobility is a gross exaggeration.

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 something to "catch" the unsuspecting pedestrian. 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.[115] 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.

---

[112] See *Pepsico*, note 106 supra, at 1270. The court explained that "Pepsico finds itself in the position of a coach, one of whose players has left, playbook in hand, to join the opposing team before the big game."

[113] See Pooley, *Trade Secrets*, note 12 supra, at §7.02[2][ii] (extensive discussion and examples of court decisions addressing "inevitable disclosure" or "threatened misappropriation").

[114] The Defend Trade Secrets Act of 2015, S. 1890, 114th Cong. §2(b)(3)(A)(1): "provided the order does not prevent a person from accepting an offer of employment under conditions that avoid actual or threatened misappropriation."

[115] 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; 14 U.L.A. 433 §§2(b), 3(a). See also note 21 supra and accompanying text.

This is a reflection of the profound differences between patents and secrets. Patents are territorial rights 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."[116] 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" in relation to patents.[117]

The pending bills would not alter these fundamental facts nor would they reduce any of the sanctions that have typically been applied to discourage frivolous claims.[118] Apart from providing a very circumscribed and risky opportunity to request ex parte seizure as described above, the only difference would be 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 we have never 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, we have been offered only opinion ("the capabilities of trade secret trolls remain to be seen, but the risk is very real")[119] and apocalyptic speculation ("trade secret trolls [will] roam free in a confused and unsettled environment, threatening or initiating

[116] 14 U.L.A. 433 §1(1). Another important distinction from patents, not specifically relevant to this point, is that the trade secrets rights flow with the information across borders, and are nominally enforceable wherever jurisdiction over the breach has been established. I say "nominally" 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, *Uncovering Trade Secrets – An Empirical Assessment of Economic Implications of Protection for Undisclosed Data* (OECD 2014), available at http://www.oecd-ilibrary.org/trade/uncovering-trade-secrets-an-empirical-assessment-of-economic-implications-of-protection-for-undisclosed-data_5jxzl5w3j3s6-en?crawler=true.

[117] See *Kewanee*, note 14 supra, at 489-90.

[118] The bills allow fee-shifting for bringing a claim of misappropriation in "bad faith," using exactly the same language as the UTSA. The Defend Trade Secrets Act of 2015, S. 1890, 114th Cong. §2(b)(3)(D); 14 U.L.A. 433 §4. If "trade secret trolls" have not sprung to life in any of the 48 states that have established this negative incentive, why would anyone imagine that it would be easier to get a frivolous case past a federal judge, who also can impose sanctions under FRCP Rule 11?

[119] See *Trolls*, note 8 supra, at 235.

lawsuits for the sole purpose of exacting settlement payments, just like patent trolls").[120]

CONCLUSION

The Defend Trade Secrets Act meets a compelling need for effective protection of information assets in the digital age. Its proposed amendments to the EEA are modest and procedural. Its language draws from existing laws. It will not preempt any 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 to protect those assets. At the same time, technology has exposed industrial secrets to unprecedented levels of risk. It is past time that the creators and owners are given the same access to federal courts that they enjoy for their other intellectual property.

The pending legislation enjoys unusually bipartisan and bicameral political support. Industry is virtually unanimous on the issue. In response to concerns about a previous version in the 113th Congress, modifications have been made to reinforce protections against abuse. The remaining objections are conjectural, and do not outweigh the clear benefits of correcting this anomaly in our intellectual property laws. Congress should approve the Defend Trade Secrets Act of 2015.

[120] *Id.* at 252.