

A D D E N D U M
to
PROTECTING TRADE SECRETS: THE IMPACT
OF TRADE SECRET THEFT ON AMERICAN
COMPETITIVENESS AND POTENTIAL
SOLUTIONS TO REMEDY THIS HARM

This Addendum is available at:

<https://www.govinfo.gov/content/pkg/CHRG-114shrg52555/pdf/CHRG-114shrg52555-add1.pdf>

Submitted by Senator Cornyn office:

Defend Trade Secrets	2
Santa Clara University School of Law	8
Various Professors, Letter	15

Submitted by Senator Grassley office:

American Bar Association	38
American Intellectual Property Law Association	40
Corporate Counsel	42
Intellectual Property Owners Association (IPO)	46
Krotoski, Mark L., Statement	47
National Alliance for Jobs and Innovation	99
Organizations for Support of Defend Trade Secrets Act	101
Sigall, Jule, Letter	104
The Recorder	106

Submitted by Senator Leahy office:

Defend Trade Secrets Act	110
--------------------------------	-----

August 3, 2015

VIA EMAIL TO THE SPONSORS OF THE DEFEND TRADE SECRETS ACT

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Signed,²

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

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

Attachments

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



Santa Clara University School of Law

Legal Studies Research Papers Series

Accepted Paper No. 35-14, September 2014

DO WE NEED A NEW FEDERAL TRADE SECRET LAW?

Eric Goldman
Santa Clara University School of Law

This paper can be downloaded without charge from the
Social Science Research Electronic Paper Collection:
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2498323

Do We Need a New Federal Trade Secret Law?

By Eric Goldman*

September 19, 2014

Trade secrets usually don't grab headlines the way that patents or copyrights do, but don't let that fool you about their importance. Studies regularly show that most businesses care more about trade secrets than either copyrights or patents.¹ In fact, trade secrets are implicated by every aspect of a company's operations, including dealings with employees, vendors and customers. And while there are millions of issued patents and registered copyrights, the total number of protectable trade secrets is nearly infinite.

Due to the qualitative and quantitative importance of trade secrets to our economy, our regulatory approach to trade secrets can have major consequences—both good and bad. Thus, you'd think that if Congress were contemplating a major change to trade secret law, that would be big news that would garner close media attention. Yet, in perhaps the most important pending legislation you aren't (currently) paying attention to, Congress is in fact currently considering two bills to create an entirely new federal law protecting trade secret rights.

This Essay will contextualize the bills, outline some questions about the needs for the bills at all, and closely analyze a new and problematic proposed ex parte seizure provision.

The Current State of Trade Secret Protection

Trade secrets are principally protected under state law, not federal law. 47 states² have adopted a model law called the Uniform Trade Secret Act (UTSA).³ However, adoptions of the UTSA are not exactly uniform.⁴ State laws typically provide both civil and criminal remedies.

Many states also have laws governing employer restrictions on employee mobility, an issue inextricably linked with trade secret protection because employee interactions generate many trade secret issues. These laws differ widely among the states. For example, many states enforce

* Professor of Law and Co-Director, High Tech Law Institute, Santa Clara University School of Law. <http://www.ericgoldman.org>; egoldman@gmail.com. An earlier version of this essay was first published as Eric Goldman, *Congress Is Considering A New Federal Trade Secret Law. Why?*, FORBES TERTIUM QUID, Sept. 16, 2014, <http://www.forbes.com/sites/ericgoldman/2014/09/16/congress-is-considering-a-new-federal-trade-secret-law-why/>. Thanks to Venkat Balasubramani, David Levine, Sharon Sandeen and Chris Seaman for comments on earlier drafts.

¹ See, e.g., John E. Jankowski, *Business Use of Intellectual Property Protection Documented in NSF Survey*, NSF 12-307 (Feb. 2012). <http://www.nsf.gov/statistics/infbrief/nsf12307/>. See generally David S. Almeling, *Seven Reasons Why Trade Secrets Are Increasingly Important*, 27 BERKELEY TECH. L.J. 1091 (2012).

² Trade Secret Act, Uniform Law Commission, <http://www.uniformlaws.org/Act.aspx?title=Trade+Secrets+Act> (visited Sept. 18, 2014).

³ Uniform Trade Secrets Act With 1985 Amendments, approved Feb. 11, 1986, http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf.

⁴ See, e.g., Warrington S. Parker III & Daniel D. Justice, *The Differing Approaches To Preemption Under The Uniform Trade Secrets Act*, 49 TORT TRIAL & INS. PRAC. L.J. 645, 646 (2014) ("Although all but three states have enacted the UTSA, uniformity has remained elusive. States have enacted slightly varying versions of the UTSA, and courts have not interpreted these statutes in a uniform manner").

employee non-competition agreements containing reasonable restrictions,⁵ while California categorically prohibits such provisions.⁶

The principal federal trade secret law is the Economic Espionage Act (EEA),⁷ a criminal law focused on corporate espionage by foreign governments. The US Department of Justice only brings a few Economic Espionage Act prosecutions a year,⁸ but the FBI has an “Economic Espionage Unit” dedicated to enforcing the law.⁹

In addition to the EEA, the federal Computer Fraud & Abuse Act (CFAA)¹⁰ prohibits misuse of a third party’s computers. It wasn’t designed as a trade secret protection law, but it’s frequently invoked in trade secret-like disputes—especially when employers allege that a departing employee misused the employer’s computers during or after their departure.¹¹ The CFAA provides both criminal and civil remedies.

The Proposed Bills

As this overview of existing law indicates, trade secret owners don’t currently have a federal civil cause of action for trade secret misappropriation. For several years, bills have been introduced into Congress to fill this perceived gap.¹² Those bills have gone nowhere, but they have helped coalesce a growing coalition of supporters for a new federal law.

The latest iterations are the Trade Secrets Protection Act of 2014 in the House (H.R. 5233)¹³ with a bi-partisan list of co-sponsors;¹⁴ and the Defend Trade Secrets Act of 2014 in the Senate (S. 2267),¹⁵ sponsored by Sens. Coons (D-DE) and Hatch (R-UT). Both bills substantially follow the UTSA’s language, although the textual differences could create confusion because the UTSA’s

⁵ See, e.g., Michael J. Garrison & John T. Wendt, *The Evolving Law Of Employee Noncompete Agreements: Recent Trends And An Alternative Policy Approach*, 45 AM. BUS. L.J. 107 (2008).

⁶ Cal. Bus. & Prof. Code § 16600.

⁷ Economic Espionage Act of 1996 (Pub. L. 104–294, 110 Stat. 3488, enacted October 11, 1996), *codified at* 18 U.S.C. §§ 1831–1839.

⁸ See Peter J. Toren, *A Look At 16 Years Of EEA Prosecutions*, Law360, Sept. 19, 2012, <http://www.law360.com/articles/378560/a-look-at-16-years-of-eea-prosecutions> (calculating that there were 124 indictments in the first 16 years of the act).

⁹ See, e.g., Christopher Munsey, *Economic Espionage: Competing For Trade By Stealing Industrial Secrets*, FBI LAW ENFORCEMENT BULLETIN, Nov. 6, 2013, <http://leb.fbi.gov/2013/october-november/economic-espionage-competing-for-trade-by-stealing-industrial-secrets>.

¹⁰ 18 U.S.C. § 1030.

¹¹ See, e.g., *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012); *US v. Nosal*, 676 F.3d 854 (9th Cir. 2012); see also Eric Goldman, *The Computer Fraud and Abuse Act Is a Failed Experiment*, FORBES TERTIUM QUID, Mar. 28, 2013, <http://www.forbes.com/sites/ericgoldman/2013/03/28/the-computer-fraud-and-abuse-act-is-a-failed-experiment/>.

¹² *Latest Updates on Federal Trade Secrets Legislation*, Trading Secrets Blog, <http://www.tradesecretslaw.com/latest-update-on-federal-trade-secret-legislation/> (visited Sept. 18, 2014).

¹³ H.R.5233 - Trade Secrets Protection Act of 2014, 113th Congress (2013-2014), <https://beta.congress.gov/bill/113th-congress/house-bill/5233/text>.

¹⁴ As of Sept. 18, 2014, there were 21 co-sponsors, including 14 Republicans and 7 Democrats. <https://beta.congress.gov/bill/113th-congress/house-bill/5233/cosponsors> (visited Sept. 18, 2014).

¹⁵ S.2267 - Defend Trade Secrets Act of 2014, 113th Congress (2013-2014), <https://beta.congress.gov/bill/113th-congress/senate-bill/2267/text>.

large corpus of interpretative precedents wouldn't help. Further, both bills would create a brand new ex parte seizure provision that doesn't have an equivalent in the UTSA (more on that shortly). Also, the bills are quite similar to each other; the House bill has a slightly narrower scope of claims, extra limitations on the ex parte seizure mechanism, and more specificity about pre-enactment claims.¹⁶

Behind the scenes, the bills are being supported by a small handful of large businesses that own a lot of trade secrets. Curiously, even though trade secrets play a crucial role in the Silicon Valley economy—in many ways, bigger than patents—Silicon Valley companies have been conspicuously silent about the bills. In fact, I believe most Silicon Valley companies—and, frankly, just about everyone outside the Beltway—have no idea these bills exist.

If the bills pass, most trade secret owners get more enforcement choices: they can sue in state court (as they always have been able to do) or they can choose federal court; and they can choose to assert state law claims, federal law claims, or both. The net consequence is that trade secret owners will win more cases.

Do We Need A New Federal Trade Secret Law?

While the bill supporters obviously would enjoy having more legal tools that help them win more enforcement actions, it's not otherwise clear what problem the proposed bills are designed to solve. The UTSA is already the law of the land, and the bills largely track the UTSA. To the extent the bills simply replicate the current state law, then what's the point?

One possible justification could be that the bills would eliminate state variations in the UTSA. That way, the federal law could establish a truly uniform national law. However, the bills explicitly say that they don't preempt state laws.¹⁷ Thus, the bills would preserve all of the existing state law complexity—and then exacerbate the complexity by creating new legal rules that will require a new body of judicial interpretations. Collectively, the extra complexity is likely to increase litigation costs for both plaintiffs and defendants, with little countervailing benefits.

Another possible justification is that the bills will ensure that trade secret owners always have the option to sue in federal court, reversing the historic dominance of trade secret cases in state court. However, trade secret owners already often find a basis to sue in federal courts if they want it (for example, due to diversity jurisdiction, or because the plaintiffs tack on a CFAA claim). Moving trade secret cases from state to federal court also has cost implications. Can the federal court system handle the new workload without additional funds? If guaranteed access to federal court is the desired goal, it's not clear how valuable that really is.

¹⁶ *Latest Updates on Federal Trade Secrets Legislation*, Trading Secrets Blog, <http://www.tradesecretslaw.com/latest-update-on-federal-trade-secret-legislation/> (visited Sept. 18, 2014).

¹⁷ Both bills say “Nothing in the amendments made by this section shall be construed to modify the rule of construction under section 1838 of title 18, United States Code, or to preempt any other provision of law” (emphasis added).

Perhaps the goals of the proposed bills are to do something beyond the UTSA's current reach. For example, much of the rhetoric supporting the proposed bills relates to fears about Chinese espionage.¹⁸ However, the Economic Espionage Act already applies to that problem.¹⁹ If the concerns about Chinese snooping are legitimate (and not just typical inside-the-Beltway scare tactics), perhaps we need more enforcement of existing laws rather than a new law.

Some of the supporting rhetoric also relates to cybersecurity concerns about bad hackers.²⁰ However, trade secret law is an ill-fitting solution for cybersecurity problems—especially in comparison with the Computer Fraud & Abuse Act, which is optimized for cybersecurity and is being used (and already misused) in that context. As Zoe Argento recently wrote:

Strengthening trade secret law, however, will likely do little to combat cyber-misappropriation....trade secret holders cannot and will not pursue cyber-misappropriators in court for technological and business reasons, not for legal reasons....the political rhetoric ignores the fact that the costs outweigh the benefits of bolstering trade secret law to respond to cyber-misappropriation of trade secrets.²¹

For a more thorough deconstruction of the purported reasons for a federal trade secret civil cause of action, see Chris Seaman's forthcoming article²² and a recent letter by David Levine and Sharon Sandeen and signed by over 30 professors (which I joined).²³

So exactly what's the problem that a federal trade secret law solves, and is it the right solution to that problem? Given the confusing rhetorical hyperbole, and the solid foundation of existing laws already on the books, the answers to those questions aren't clear.

The Ex Parte Seizure Provision

The bills' most significant departure from the UTSA is a proposed new ex parte seizure provision. The UTSA does not explicitly provide an equivalent procedure, though civil procedure law provides several mechanisms for plaintiffs to obtain quick relief, including ex parte temporary restraining orders (TROs) in extraordinary circumstances.

¹⁸ *Latest Updates on Federal Trade Secrets Legislation*, Trading Secrets Blog, <http://www.tradesecretslaw.com/latest-update-on-federal-trade-secret-legislation/> (visited Sept. 18, 2014).

¹⁹ Toren, *supra* note 8 ("more than 20 percent of all of the [EEA] prosecutions involved Chinese citizens or naturalized U.S. citizens originally from China. In addition, in slightly less than 30 percent of the total EEA prosecutions, the defendant misappropriated the trade secrets to benefit the Chinese government, an existing Chinese company or to start a company there. [¶] The trend of a China connection is also increasing.")

²⁰ *Latest Updates on Federal Trade Secrets Legislation*, Trading Secrets Blog, <http://www.tradesecretslaw.com/latest-update-on-federal-trade-secret-legislation/> (visited Sept. 18, 2014).

²¹ 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, 177 (2014).

²² Christopher B. Seaman, *The Case Against Federalizing Trade Secrecy*, __ VIRGINIA L. REV. __ (forthcoming), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2397567.

²³ 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), Aug. 26, 2014, <https://s3.amazonaws.com/ftt-uploads/tradesecretletter2014.pdf>.

Why would trade secret owners want an ex parte seizure provision? “Ex parte” means that the trade secret owner appears in court, alone, to tell its story to the judge. In other words, the judge only hears one side of a story, even though the “full” story could be complex and contentious. As a result, the seizure provision would allow trade secret owners to go to court, unopposed, and obtain a court order to grab some of their competitors’ stuff. (The House bill is vague about exactly what stuff can be grabbed: it allows “the seizure of property necessary to preserve evidence...or to prevent the propagation or dissemination of the trade secret that is the subject of the action.”)

In practice, the provision effectively could let trade secret owners take competitors out of the marketplace for a period of time. I think this would be an especially attractive tactic as a parting gift for former employees who go to competitors or try to start up a new competing venture. The threat of a seizure, issued behind closed doors without the target’s knowledge, is a menacing tool that can be easily misused to abuse departing employees and competitors who want to hire them.

The House bill (and to a much lesser extent, the Senate bill) provides some checks and balances to reduce the risk that trade secret owners would misuse the ex parte seizure. However, no matter how strong those checks and balances are, I don’t believe it’s possible to salvage the concept of a new ex parte seizure procedure for two principal reasons.

First, we know that ex parte proceedings routinely go wrong in other IP contexts. For example, the US government has been seizing domain names on an ex parte basis, which has led to several egregious mistakes.²⁴ In the civil context, IP owners who’ve sought ex parte relief frequently ask for—and get the judge to grant them—obviously overbroad relief.²⁵ These all-too-common errors occur because judges expect to hear two or more sides of a story. When presented with only one side’s arguments, judges systematically overweight the plaintiff’s un rebutted assertions and don’t adequately research the facts or the law to identify otherwise obvious deficiencies.

Second, trade secrets lawsuits frequently involve disputes about (1) whether the plaintiff actually has an enforceable trade secret, i.e., if the information qualifies for a trade secret, and (2) if the plaintiff actually owns the rights. Unlike patents, copyrights and (for the most part) trademarks, there’s no government registry of trade secrets that courts can consult or defer to. Further, it’s easy for information to lose trade secret status, and the purported owner may not even realize that has occurred. As a result, a typical trade secret case will involve a bitter fight over whether information still qualifies as a trade secret.

This means we simply cannot take competition-distorting actions based on a purported owner one-sided claims to own trade secrets; those self-interested assertions are too likely to be wrong or overstated, even if made in “good faith.” Instead, the only reliable way to know if information qualifies as a trade secret is to hear another side of the story from a financially motivated

²⁴ See, e.g., Karen Kopel, *Operation Seizing Our Sites: How The Federal Government Is Taking Domain Names Without Prior Notice*, 28 BERKELEY TECH. L.J. 859 (2013).

²⁵ See, e.g., Venkat Balasubramani, *Hermès Obtains (Ex Parte) \$100M Award Against Alleged Counterfeiters—Hermès v. Does*, Technology & Marketing Law Blog, May 2, 2012, http://blog.ericgoldman.org/archives/2012/05/hermes_obtains.htm.

adversarial party. By definition, ex parte proceedings categorically cannot achieve this level of reliability because there's no adversarial party at all.

The bills effectively ignore the "is there a trade secret?" problem. In the House bill, the plaintiff simply needs to show that it "is likely to succeed in showing that the person against whom seizure would be ordered misappropriated the trade secret and is in possession of the trade secret." The Senate bill is completely silent on the issue.

We could try to fix the bills to better address the trade secret existence/ownership problem, but there's no way to fix the problem adequately. As a result, the only logical solution is to remove the ex parte seizure provisions from the proposals entirely, directing trade secret owners to rely on existing civil procedure mechanisms rather than getting a new expedited fast lane. So long as the ex parte seizure language remains, the bills are fatally problematic.

Conclusion

Even if the ex parte seizure provisions are stripped out (as they should be), the proposed bills have complicated implications for our trade secret regulatory scheme. The burden of persuasion should rest with the bills' proponents to give us a clear and concise explanation for why the bills are needed. The proponents have not met that burden of persuasion yet.

Professors' Letter in Opposition to the Defend Trade Secrets Act of 2015
(S. 1890, H.R. 3326)

November 17, 2015

The Honorable Charles E. Grassley
Chairman
Judiciary Committee
United States Senate
224 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Robert W. Goodlatte
Chairman
Judiciary Committee
United States House of Representatives
2138 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Patrick J. Leahy
Ranking Member
Judiciary Committee
United States Senate
224 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable John Conyers, Jr.
Ranking Member
Judiciary Committee
United States House of Representatives
B-251 Rayburn House Office Building
Washington D.C. 20515

Dear Chairmen Grassley and Goodlatte, and Ranking Members Leahy and Conyers:

In August 2014, thirty-one law professors signed a letter in opposition to proposed federal legislation to create a civil cause of action for trade secret misappropriation.¹ We write to express continued concerns about the current version of this legislation, the Defend Trade Secrets Act of 2015 (“DTSA”), S. 1890 and H.R. 3326.² While we agree that effective legal protection for U.S. businesses’ legitimate trade secrets is important to American innovation, we believe that the DTSA—which would represent the most significant expansion of federal law in intellectual property since the Lanham Act in 1946—will not solve the problems identified by its sponsors. Instead of addressing cyberespionage head-on, passage of the DTSA is likely to create new problems that could adversely impact domestic innovation, increase the duration and cost of trade secret litigation, and ultimately negatively affect economic growth. **Therefore, the undersigned call on Congress to reject the DTSA.**

¹ Professors’ Letter in Opposition to the “Defend Trade Secrets Act of 2014” (S. 226) and the “Trade Secrets Protection Act of 2014” (H.R. 5233) (Aug. 26, 2014), *available at* <http://cyberlaw.stanford.edu/files/blogs/FINAL%20Professors%20Letter%20Opposing%20Trade%20Secret%20Legislation.pdf> [hereinafter “2014 Professors’ Letter”] and attached. This letter incorporates and expands upon the concerns raised in the 2014 Professors’ Letter.

² We understand that the House and Senate versions of this legislation are now substantively identical. For convenience, this letter cites to the provisions of the Senate version, S. 1890, 114th Cong. (2015) as introduced on July 29, 2015 [hereinafter “S. 1890”].

Professors' Letter in Opposition to the Defend Trade Secrets Act of 2015
(S. 1890, H.R. 3326)

Summary of Arguments

In recent years, numerous concerns about a federal civil cause of action for trade secret misappropriation have been detailed in analyses prepared by experts in the field of trade secret and intellectual property law.³ Fundamentally, these experts oppose the legislation because: (1) it will not address the cyberespionage problem that is most often used to justify the adoption of a federal trade secret law; (2) a federal trade secret law is not needed to protect U.S. trade secrets because there is already a robust set of state laws for the protection of such secrets; and (3) there are significant costs to creating a federal civil cause of action for trade secret misappropriation. In addition to these concerns, this letter details the following four specific reasons why the undersigned urge rejection of the 2015 Defend Trade Secrets Act.

1. **The DTSA's *Ex Parte* Seizure Provision May Harm Small Businesses, Startups and Other Innovators**
2. **The DTSA Appears to Implicitly Recognize The Inevitable Disclosure Doctrine**
3. **The DTSA Likely Will Increase the Length and Cost of Trade Secret Litigation**
4. **The DTSA Will Likely Result in Less Uniformity in Trade Secret Law**

We also urge Congress to **hold hearings** that focus on the costs of the legislation and whether the DTSA addresses the cyberespionage problem that it is allegedly designed to combat. Specifically, Congress should evaluate the DTSA **through the lens of employees, small businesses, and startup companies** that are most likely to be adversely affected by the legislation.

³ Contrary to the assertion that there is no opposition to the DTSA, a number of scholars and commentators have raised concerns about the DTSA's scope, efficacy and impact. See Eric Goldman, *Federal Trade Secret Bill Re-Introduced—And It's Still Troublesome*, Technology & Marketing Law Blog, <http://blog.ericgoldman.org/archives/2015/08/federal-trade-secret-bill-re-introduced-and-its-still-troublesome-guest-blog-post.htm> (Aug. 4, 2015); David S. Levine & Sharon K. Sandeen, *Open Letter to the Sponsors of the Revised Defend Trade Secrets Act*, <http://cyberlaw.stanford.edu/publications/open-letter-sponsors-revised-defend-trade-secrets-act> (Aug. 3, 2015); John Tanski, *The Defend Trade Secrets Act is Strong Medicine. Is It Too Strong?*, Nat'l L.J., Oct. 30, 2015, <http://www.law.com/lls/sites/articles/2015/10/30/the-defend-trade-secrets-act-is-strong-medicine-is-it-too-strong/?slreturn=20150931104239>. Additional recent scholarship critical of proposals to create a federal civil cause of action for trade secret misappropriation include: Zoe Argento, *Killing the Golden Goose: The Dangers of Strengthening Domestic Trade Secret Rights In Response to Cyber-Misappropriation*, 16 Yale J.L. & Tech. 172 (2014); David S. Levine & Sharon K. Sandeen, *Here Come the Trade Secret Trolls*, 71 Wash. & Lee L. Rev. Online 230 (2015); Christopher B. Seaman, *The Case Against Federalizing Trade Secrecy*, 101 Va. L. Rev. 317 (2015).

Professors' Letter in Opposition to the Defend Trade Secrets Act of 2015
(S. 1890, H.R. 3326)

Detailed Arguments

1. The DTSA's *Ex Parte* Seizure Provision May Harm Small Businesses, Startups and Other Innovators

Like its predecessor bills, the current version of the DTSA contains a controversial provision authorizing a trade secret owner to obtain, on an *ex parte* basis, a court order to seize property that contains alleged trade secret information under certain circumstances.⁴ Although this provision is more limited in scope than prior proposals,⁵ it still contains significant potential to cause anti-competitive harm, particularly against U.S.-based small businesses, startups and other entrepreneurs. Moreover, proponents of the DTSA have argued that such a provision will not be frequently utilized, which raises the question: Why create a new remedy that is fraught with potential for abuse?

First, the DTSA's *ex parte* seizure provision is impermissibly vague. It is unclear from the statutory text what "property" may be seized "to prevent the propagation or dissemination" of the alleged trade secret. For example, if the alleged trade secret is computer source code, could the court order the seizure of all computer servers (and other electronic storage media, like flash drives) under the defendants' control that contains a copy of the code? Even with the requirement that the *ex parte* seizure order must "provide for the narrowest seizure of property necessary to achieve [these] purposes,"⁶ it may still result in significant harm to the alleged misappropriator's legitimate business operations.⁷

Second, the *ex parte* nature of the process for obtaining a seizure order means that an alleged misappropriator will be unable to immediately and meaningfully challenge the plaintiff's assertions regarding the alleged trade secret status of the information and the claimed misappropriation. As one commentator recently explained, "so much business information can potentially qualify as a trade secret that it is easy for unscrupulous plaintiffs

⁴ S. § 1890, § 2 (proposed for codification at 18 U.S.C. § 1836(b)(2)). For a more detailed critique of the infirmities of the *ex parte* seizure provision, see Eric Goldman, *Ex Parte Seizures and the Defend Trade Secrets Act*, 72 Wash. & Lee L. Rev. Online (forthcoming Nov. 2015).

⁵ Among other changes, the current version of the *ex parte* seizure provision would limit the scope of a seizure order to "property necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action," *id.* (proposed for codification at 18 U.S.C. § 1836(b)(2)(A)(i)); it would add additional details regarding the required court hearing within seven days after the *ex parte* seizure is granted, *id.* (proposed for codification at 18 U.S.C. § 1836(b)(2)(F)); and it would require that the court take possession of the seized materials, *id.* (proposed for codification at 18 U.S.C. § 1836(b)(2)(D)). Like last year's DTSA, it also includes a provision allowing for an action for damages in the case of wrongful seizure. *Id.* (proposed for codification at 18 U.S.C. § 1836(b)(2)(G)).

⁶ *Id.* (proposed for codification at 18 U.S.C. § 1836(b)(2)(B)(ii)).

⁷ *Cf.* *Steve Jackson Games, Inc. v. U.S. Secret Service*, 816 F. Supp. 432 (W.D. Tex. 1993), *aff'd on other grounds*, 36 F.3d 457 (5th Cir. 1994) (seizure of computer server allegedly containing an item of stolen information caused significant collateral damage that permanently undermined the company's business).

Professors' Letter in Opposition to the Defend Trade Secrets Act of 2015
(S. 1890, H.R. 3326)

to manufacture trade secret claims and use them as strategic weapons.”⁸ Self-interested advocates seeking an *ex parte* seizure order are unlikely to point out potential weaknesses and/or complexities in their own case, such as the likelihood of reverse engineering and previous disclosures that may undermine the claim of secrecy. Indeed, because the defendant is absent from the courtroom, the court will lack knowledge of any relevant facts that would weigh against granting a seizure. As a result, the DTSA’s *ex parte* seizure provision is particularly pro-plaintiff.

Critically, because opposing an *ex parte* seizure order “is likely to be an extremely expensive process for both the courts and the parties, start-up companies that are sued by larger companies might very well capitulate rather than incur the expense” of challenging the plaintiff’s claims.⁹ As a result, “[t]he chilling effect on innovation and job growth . . . could be profound.”¹⁰ Especially as the DTSA fails to meaningfully address the cyberespionage problem repeatedly cited by its proponents, this reason alone suggests it should be rejected.¹¹

2. The DTSA Appears to Implicitly Recognize The Inevitable Disclosure Doctrine

The current version of the DTSA also contains new language regarding injunctive relief that appears to implicitly recognize the so-called inevitable disclosure doctrine. If accurate, this would represent a profound shift in both the law governing the enforceability of non-compete agreements and trade secrets, particularly in jurisdictions that do not currently recognize the doctrine.

Under the inevitable disclosure doctrine, “a plaintiff may prove a claim of trade secret misappropriation by demonstrating that defendant’s new employment will inevitably lead him to rely on the plaintiff’s trade secrets.”¹² “Inevitable disclosure is not a separate cause of action; rather, it is a means of proving misappropriation or irreparable harm for injunctive relief.”¹³ In states that recognize inevitable disclosure, the typical remedy is to enjoin the

⁸ Tanski, *supra* note 3.

⁹ Levine & Sandeen, *Open Letter to the Sponsors of the Revised Defend Trade Secrets Act*, *supra* note 3, at 2.

¹⁰ Levine & Sandeen, *Here Come the Trade Secret Trolls*, *supra* note 3, at 255; *see also* Tanski, *supra* note 3 (explaining that “[t]he DTSA’s seizure provision—which effectively allows the plaintiff to petition the court, in secret, to shut down the defendant’s business for up to a week—creates significant business risk”). Importantly, other avenues for preliminary relief would still remain open to trade secret holders, including temporary restraining orders (TROs), preliminary injunctions, takedown notices under the Digital Millennium Copyright Act, and *ex parte* seizures under the Lanham Act.

¹¹ For further discussion of the DTSA’s negative impact on cybersecurity and its failure to address cyberespionage, *see* David S. Levine, *School Boy’s Tricks: Reasonable Cybersecurity and the Panic of Law Creation*, 72 Wash & Lee L. Rev. Online (forthcoming 2015).

¹² *PepsiCo, Inc. v. Redmond*, 54 F.3d 1262, 1269 (7th Cir. 1995).

¹³ Seaman, *supra* note 3, at 366.

Professors' Letter in Opposition to the Defend Trade Secrets Act of 2015
(S. 1890, H.R. 3326)

departing employee from commencing employment until the subject trade secret information is no longer a trade secret. As Professor Elizabeth Rowe has explained, “[t]he inevitable disclosure doctrine is controversial primarily because . . . at its core, it appears to go against a fundamental tenet of employment law: the at-will doctrine.”¹⁴

The current version of the DTSA contains language that could reasonably be interpreted to endorse the inevitable disclosure doctrine as a matter of federal law. The DTSA provides that a court may grant an injunction “to prevent any actual or threatened misappropriation . . . on such terms as the court deems reasonable, *provided the order does not prevent a person from accepting an offer of employment under conditions that avoid actual or threatened misappropriation.*”¹⁵ The italicized language implies that if there are no conditions that would effectively prevent a departing employee from engaging in “actual or threatened misappropriation” once he or she has started working for a new employer, then the district court may grant an injunction prohibiting the employee from accepting the new position.

Federal recognition of the inevitable disclosure doctrine would be troubling because “a rising number of empirical studies . . . suggest that lesser constraints on employee mobility may increase economic growth and innovation.”¹⁶ It would also contradict the long-standing public policy of jurisdictions like California that reject the inevitable disclosure doctrine as a matter of state law, and that have benefitted greatly from employee mobility.¹⁷ In such jurisdictions, trade secret holders seeking an injunction against departing employees would simply invoke federal law, thus effectively rendering the state law inoperative. In sum, the risk that putative trade secret holders—particularly incumbent firms—could prevent individuals from being able to feed their families through this controversial doctrine, and also misuse this provision against small businesses and startups, counsel rejection of the DTSA.

3. The DTSA Likely Will Increase the Length and Cost of Trade Secret Litigation

In addition, the DTSA likely will increase the length and cost of trade secret litigation, thus further exacerbating the DTSA’s negative impact on small businesses and startups. Specifically, the DTSA would grant federal courts original (but not exclusive) jurisdiction

¹⁴ Elizabeth A. Rowe, *When Trade Secrets Become Shackles: Fairness and the Inevitable Disclosure Doctrine*, 7 Tul. J. Tech. & Intell. Prop. 167, 183 (2005).

¹⁵ S. 1890, § 2 (proposed for codification at 18 U.S.C. § 1836(b)(3)) (emphasis added).

¹⁶ On Amir & Orly Lobel, *Driving Performance: A Growth Theory of Noncompete Law*, 16 Stan. Tech. L. Rev. 833, 837-38 (2013).

¹⁷ See *Whyte v. Schlage Lock Co.*, 125 Cal. Rptr. 2d 277, 291-94 (Ct. App. 2002) (rejecting inevitable disclosure under California law).

Professors' Letter in Opposition to the Defend Trade Secrets Act of 2015
(S. 1890, H.R. 3326)

over civil trade secret claims.¹⁸ To establish federal jurisdiction, a trade secret plaintiff suing under the DTSA would have to show that the alleged trade secret is “related to a product or service used in, or intended for use in, interstate or foreign commerce.”¹⁹ Although this provision is apparently broad in scope, “it obviously does not (and cannot) describe all U.S. trade secret information, as not all trade secrets are necessarily ‘related to a product or service . . . used in . . . commerce,’ like many customers lists.”²⁰ At a minimum, the trade secret plaintiff would have to demonstrate to the court’s satisfaction, likely early in the case, that the alleged trade secrets satisfy this jurisdictional requirement which is demanded by the Commerce Clause of the U.S. Constitution. This would both delay the case and result in increased costs in litigating the issue.

Another reason that the DTSA may increase the cost of trade secret litigation is the broad scope of discovery permitted under the Federal Rules of Civil Procedure. Discovery in trade secret litigation is already very expensive; a recent survey of IP lawyers found that median litigation costs through the end of discovery ranged from \$250,000 in cases where less than \$1 million was at stake, to over \$1.6 million in cases where over \$25 million was at risk.²¹ The stringent pleading requirements and liberal discovery standards of federal courts, and electronic discovery, may exacerbate this problem. These cost concerns also call for the DTSA’s abandonment.

4. The DTSA Will Likely Result in Less Uniformity in Trade Secret Law

Lastly, DTSA’s sponsors contend that its adoption would “[h]armonize U.S. law” and “create a uniform standard for trade secret misappropriation.”²² Yet, in reality, the law would be adopted against the backdrop of the non-existence of any federal jurisprudence regarding a civil trade secret claim.²³ Moreover, a careful examination of the bill’s provisions, reveal that the DTSA would in fact result in *less* uniformity in trade secrets law than currently exists.

¹⁸ S. 1890, § 2 (proposed for codification at 18 U.S.C. § 1836(c)). For a fuller discussion of these issues, see Sharon K. Sandeen, *DTSA: The Litigator's Full-Employment Act*, 72 Wash & Lee L. Rev. Online (forthcoming 2015).

¹⁹ *Id.* (proposed for codification in 18 U.S.C. § 1836(b)(1)).

²⁰ 2014 Professors’ Letter, *supra* note 1, at 3.

²¹ Am. Intellectual Prop. Law Ass’n, Report of the Economic Survey 2015, at 39, I-166, I-169 (2015).

²² Press Release, Senate, House Leaders Introduce Bipartisan, Bicameral Bill to Protect Trade Secrets (July 29, 2015), <http://www.hatch.senate.gov/public/index.cfm/2015/7/senate-house-leaders-introduce-bipartisan-bicameral-bill-to-protect-trade-secrets>; see also Letter from Association of Global Automakers, Inc. et al., to the Honorable Orrin Hatch et al. (July 29, 2015), available at <http://www.hatch.senate.gov/public/cache/files/09ce963b-6166-4156-b924-ab1c7f4098f5/DTSA%20Senate%20Support%20Letter.pdf> (“The Defend Trade Secrets Act will create a harmonized, uniform standard and system for companies to protect their trade secrets.”).

²³ See Sharon K. Sandeen, *The Evolution of Trade Secret Law: Why Courts Commit Error When They Do Not Follow the UTSA*, 33 Hamline L. Rev. 493(2010) (explaining that in the 1960s there were several proposals to adopt a

Professors' Letter in Opposition to the Defend Trade Secrets Act of 2015
(S. 1890, H.R. 3326)

As explained in the 2014 Professors' Letter, "[t]here is already a robust and uniform body of state law governing the protection of trade secrets in the United States."²⁴ The Uniform Trade Secrets Act ("UTSA") has been adopted by 47 of 50 states,²⁵ and many U.S. businesses have successfully used the UTSA for decades to combat trade secret misappropriation. Indeed, even advocates of a federal civil cause of action for trade secret misappropriation acknowledge that the UTSA helped create a "coherent and consistent body of trade secrets law"²⁶ that has resulted in "greater consistency in the application of trade secret law and in the laws themselves."²⁷ As a result, this well-established, substantially uniform body of law has a high level of predictability for U.S. businesses and their attorneys.

The DTSA would undermine this high degree of uniformity by creating new differences with existing state law and by requiring the development of a new body of federal jurisprudence. For example, the vast majority of states have adopted a three-year statute of limitations for aggrieved businesses and individuals to bring trade secret claims.²⁸ The DTSA has a five-year statute of limitations.²⁹ The DTSA would also accept, without change, the existing Economic Espionage Act's ("EEA") definition of a trade secret, which is broader in several respects than the UTSA.³⁰ Also, as previously mentioned, the DTSA appears to endorse a new barrier to mobility of labor by recognizing the so-called inevitable

federal trade secret law but also concerns about the absence of federal jurisprudence on the subject, thereby leading to the drafting of the UTSA instead).

²⁴ 2014 Professors' Letter, *supra* note 1, at 2; *see also* TianRui Group Co. v. Int'l Trade Comm'n, 661 F.3d 1322, 1327 (Fed. Cir. 2011) ("[T]rade secret law varies little from state to state and is generally governed by widely recognized authorities such as . . . the Uniform Trade Secrets Act.").

²⁵ *See* Seaman, *supra* note 3, at 391-92 (detailing each state's adoption of the UTSA). New York generally follows the *Restatement (Third) of Unfair Competition*, which is largely based upon the UTSA. *See Wiener v. Lazard Freres & Co.*, 241 A.D.2d 114, 124, 672 N.Y.S.2d 8, 15 (1st Dep't 1998) (applying *Restatement (Third) of Unfair Competition* to define a trade secret in New York). Massachusetts trade secret law is based in small part on statutory law and in large part on common law that is consistent with what is expressed in the *Restatement (Third) of Unfair Competition*. *See* Mass. Gen. Laws Ann. ch. 93, §§ 42 to 42A and Mass. Gen. Laws Ann. ch. 266, § 30(4). North Carolina has adopted a statute that codifies many of the key principles UTSA. *See* N.C. Gen. Stat. § 66-152 *et seq.* (2014).

²⁶ 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, 670 (2008).

²⁷ David S. Almeling, *Seven Reasons Why Trade Secrets Are Increasingly Important*, 27 Berkeley Tech. L.J. 1091, 1106 (2012).

²⁸ Seaman, *supra* note 3, at 393-94.

²⁹ S. 1890, § 2 (proposed for codification at 18 U.S.C. § 1836(d)).

³⁰ Seaman, *supra* note 3, at 361-62. For discussion of the broad trade secret definition under the EEA, *see* Rochelle Dreyfuss and Orly Lobel, *Economic Espionage as Reality or Rhetoric: Equating Trade Secrecy with National Security* (on file with authors).

Professors' Letter in Opposition to the Defend Trade Secrets Act of 2015
(S. 1890, H.R. 3326)

disclosure doctrine, even though a number of UTSA jurisdictions have expressly rejected this ill-conceived doctrine.³¹

Most significantly, the DTSA expressly declines to preempt existing law regarding trade secrets because the jurisdictional requirement could not possibly cover all trade secret claims.³² This will permit a federal civil cause of action for trade secret misappropriation to exist in parallel with state law, possibly in the same lawsuit. Thus, in a trade secret dispute, the trade secret holder would seek to invoke whichever law—federal or state—appears most favorable under the circumstances. This would encourage forum-shopping and cause choice-of-law problems that are widely recognized as undesirable, and would not advance the fight against cyberespionage. This further underscores that the DTSA should be rejected.

* * *

For these reasons, the undersigned law professors **urge Congress to reject the DTSA**. In addition, as requested in the 2014 Professors' Letter,³³ we call for your Committees to **schedule full hearings** so that the informed opinions of all sides—both proponents and opponents—can be fully discussed and challenged in an open forum. Importantly, hearings should not be limited simply to denouncing cyberespionage against U.S. companies, which we agree is a problem. Rather, **the hearings should focus on the costs of the legislation, as well as whether the DTSA addresses the cyberespionage problem that it is allegedly designed to combat**. In particular, we call for Congress to **evaluate the DTSA through the lens of employees, small businesses, and startup companies that are most likely to be adversely affected by the legislation**.

You may address any reply or correspondence to its authors and organizers, Professor Eric Goldman (egoldman@gmail.com), Professor David S. Levine (dsl2@princeton.edu), Professor Sharon K. Sandeen (ssandeen@hamline.edu), and Professor Christopher B. Seaman (seamanc@wlu.edu).

³¹ See, e.g., *Whyte v. Schlage Lock Co.*, 125 Cal. Rptr. 2d 277 (Ct. App. 2002); *LeJeune v. Coin Acceptors, Inc.*, 849 A.2d 451 (Md. 2004). For further discussion of labor mobility issues in the technology sector, see AnnaLee Saxenian, *Regional Advantage: Culture and Competition in Silicon Valley and Route 128* (Cambridge, MA: Harvard University Press), 1994).

³² See S. 1890, § 2 (proposed for codification at 18 U.S.C. § 1839(f)) (“Nothing in the amendments made by this section shall be construed to . . . preempt any other provision of law.”).

³³ 2014 Professors' Letters, *supra* note 1, at 7.

Professors' Letter in Opposition to the Defend Trade Secrets Act of 2015
(S. 1890, H.R. 3326)

Respectfully submitted,*

Eric Goldman
Professor of Law
Santa Clara University School of Law

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

Sharon K. Sandeen
Professor of Law
Hamline University School of Law

Christopher B. Seaman
Associate Professor of Law
Washington and Lee University School of Law

Jane Bambauer
Associate Professor of Law
University of Arizona, James E. Rogers College of Law

Jim Bessen
Lecturer in Law
Boston University School of Law

Mario Biagioli
Distinguished Professor of Law and Science and Technology Studies
Director, Center for Science and Innovation Studies
University of California, Davis

Barbara B. Bressler
Associate Professor of Law
Director Emeritus, Center for Intellectual Property Law and Information
Technology
DePaul University College of Law

* All institutions are listed for identification purposes only. The signatories speak only for themselves, and not for or on behalf of their respective institutions or for any other entity.

Professors' Letter in Opposition to the Defend Trade Secrets Act of 2015
(S. 1890, H.R. 3326)

Irene Calboli
Professor of Law
Texas A&M University School of Law

Michael A. Carrier
Distinguished Professor of Law
Rutgers Law School

Rochelle Dreyfuss
Pauline Newman Professor of Law
New York University School of Law

Eric Fink
Associate Professor of Law
Elon University School of Law

Catherine Fisk
Chancellor's Professor of Law
Co-Director, Center in Law, Society and Culture
University of California, Irvine School of Law

William Gallagher
Professor of Law
Co-Director, IP Law Center
Golden Gate University School of Law

Elizabeth Townsend Gard
Jill. H and Avram A. Glazer Professor in Social Entrepreneurship
Co-Director, Tulane Center for IP, Media & Culture
Tulane University Law School

Shubha Ghosh
Vilas Research Fellow & George Young Bascom Professor in Business Law
University of Wisconsin Law School

Megan Gray
Non-Residential Fellow
Stanford Law School Center for Internet and Society

Camilla A. Hrdy
Fellow
Center for Technology, Innovation & Competition
University of Pennsylvania Law School

Professors' Letter in Opposition to the Defend Trade Secrets Act of 2015
(S. 1890, H.R. 3326)

Eric E. Johnson
Associate Professor of Law
University of North Dakota School of Law

Faye E. Jones
Director of the Library and Clinical Professor of Law
University of Illinois College of Law

Margot Kaminski
Assistant Professor of Law
The Ohio State University, Moritz College of Law

Yvette Liebesman
Associate Professor
Saint Louis University School of Law

Patrick Lin
Associate Professor
Cal Poly San Luis Obispo
Affiliate Scholar, Stanford Law School Center for Internet and Society

Orly Lobel
Don Weckstein Professor of Employment and Labor Law
Faculty Member, Center for Intellectual Property & Markets
University of San Diego

Lydia Loren
Robert E. Jones Professor of Advocacy and Ethics
Lewis & Clark Law School

Brian J. Love
Assistant Professor
Co-Director of the High Tech Law Institute
Santa Clara University School of Law

William Moner
Instructor
Elon University School of Communications

Deirdre Mulligan
Associate Professor, School of Information
Faculty Director, Berkeley Center for Law and Technology
University of California, Berkeley

Professors' Letter in Opposition to the Defend Trade Secrets Act of 2015
(S. 1890, H.R. 3326)

Ira Steven Nathenson
Professor of Law
St. Thomas University School of Law

Brian Nienhaus
Associate Professor of Business Communication
Elon University School of Business

Tyler T. Ochoa
Professor of Law
Santa Clara University School of Law

David Olson
Associate Professor of Law
Boston College Law School

Kenneth L. Port
Professor of Law
William Mitchell College of Law

David G. Post
Professor of Law (ret.)
Temple University, Beasley School of Law

Michael Risch
Professor of Law
Villanova University School of Law

Simone Rose
Professor of Law
Wake Forest University School of Law

Pam Samuelson
Richard M. Sherman Distinguished Professor of Law
Professor of School of Information
Co-Director, Berkeley Center for Law & Technology
University of California, Berkeley

Joshua Sarnoff
Professor of Law
DePaul University College of Law

Professors' Letter in Opposition to the Defend Trade Secrets Act of 2015
(S. 1890, H.R. 3326)

Kurt Saunders
Professor of Business Law
California State University Northridge

Katherine J. Strandburg
Alfred B. Engelberg Professor of Law
New York University School of Law

Rebecca Tushnet
Professor of Law
Georgetown University School of Law

Sally K. Wiant
Professor of Law
Washington and Lee University School of Law

**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

To the sponsors of the above-referenced legislation and other Members of the United States Congress:

The undersigned are 31 professors from throughout the United States who teach and write extensively about intellectual property law, trade secret law, innovation policy and/or information law.¹ We urge Congress to reject the proposed legislation to create a new private cause of action under the Economic Espionage Act of 1996 ("EEA"),² known as the "Defend Trade Secrets Act of 2014" ("DTSA") and the "Trade Secrets Protection Act of 2014" ("TSPA," collectively, "the Acts"). As explained in Senator Coons' press release announcing the introduction of the DTSA,

In today's electronic age, trade secrets can be stolen with a few keystrokes, and increasingly, they are stolen at the direction of a foreign government or for the benefit of a foreign competitor. These losses put U.S. jobs at risk and threaten incentives for continued investment in research and development. Current federal criminal law is insufficient.³

While we acknowledge the need to increase protection both domestically and internationally against domestic and foreign cyber-espionage, this is not the way to address those concerns. Instead, as explained below, the Acts will create or exacerbate many existing legal problems but solve none. Accordingly, we oppose their adoption.

¹ Many of the signatories to this letter also have extensive intellectual property litigation experience in state and federal courts, including trade secret litigation.

² 18 U.S.C. § 1830 *et seq.* (2014).

³ Press Release, *Senators Coons, Hatch introduce bill to combat theft of trade secrets and protect jobs*, Office of Senator Christopher Coons (April 29, 2014), available at <http://www.coons.senate.gov/newsroom/releases/release/senators-coons-hatch-introduce-bill-to-combat-theft-of-trade-secrets-and-protect-jobs>.

The Acts should be rejected for five primary reasons:

1. Effective and uniform state law already exists.

United States trade secret law was developed and is applied against a backdrop of related state laws and legal principles that reflect the values and interests of individual states, particularly with respect to issues of employee mobility and free competition. There is already a robust and uniform body of state law governing the protection of trade secrets in the United States, the Uniform Trade Secrets Act ("UTSA"), which has been adopted by 47 of 50 states.⁴ Built on over 100 years of case law, numerous US companies have used it with success to combat trade secret misappropriation by both employees and non-employees. Similarly, criminal prosecutions under the existing EEA are increasing and are addressing the concerns motivating introduction of the Acts.⁵

This deep body of state law creates its own benefits; as the general principles of US trade secret law are well-established and substantially uniform, there is a high level of predictability by and for US businesses and their attorneys. But because the Acts cannot entirely preempt state trade secret law (for reasons that are explained below), they will result in confusion, as well as less uniformity and predictability. As a result, the business community will suffer from decreased predictability in the law with, as discussed below, no corresponding benefits.

⁴ North Carolina has adopted a statute that is substantially similar to the UTSA. *See* N.C. Gen. Stat. § 66-152 *et seq.* (2014). New York generally follows the Restatement (Third) of Unfair Competition (which is largely based upon the UTSA). *See Wiener v. Lazard Freres & Co.*, 241 A.D.2d 114, 124, 672 N.Y.S.2d 8, 15 (1st Dep't 1998) (applying Restatement (Third) of Unfair Competition to define a trade secret in New York). Massachusetts trade secret law is based in small part on statutory law and in large part on common law that is consistent with what is expressed in the Restatement (Third) of Unfair Competition. *See* Mass. Gen. Laws Ann. ch. 93, §§ 42 to 42A and Mass. Gen. Laws Ann. ch. 266, § 30(4).

⁵ *See* Webinar Press Release, *Combating Trade Secret Theft: What Every Company Should Know about the EEA and CFAA*, Ballard Spahr LLP (April 24, 2014), *available at* <http://www.ballardspahr.com/eventsnews/events/2014-04-24-combating-trade-secret-theft.aspx> (asserting that "the U.S. government has made combating corporate and state-sponsored trade secret theft a top priority, and both the [Department of Justice] and [Federal Bureau of Investigation] have increased their investigations and prosecutions of it."); *see also* Indictment, *United States v. Wang Dong et al.*, Crim. No. 14-118 (W.D. Pa. May 1, 2014) (criminally charging five members of China's People's Liberation Army with economic espionage and computer hacking).

2. The Acts will damage trade secret law and jurisprudence by weakening uniformity while simultaneously creating parallel, redundant and/or damaging law.

Generally, the Commerce Clause of the United States Constitution⁶ gives Congress power to legislate trade secret law, but Congress' power is limited.⁷ To address this limitation, the Acts require a convoluted and untested jurisdictional clause that currently states that 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." While the precise meaning of this clause is unclear and unsettled, it obviously does not (and cannot) describe all US trade secret information, as not all trade secrets are necessarily "related to a product or service ... used in ... commerce," like many customer lists. Accordingly, the Acts will not supplant state law and we expect that the bulk of trade secret claims will still be based upon state law.

Moreover, even under the Acts, ancillary state law will still apply with respect to a number of important issues. Primary among them are ownership of inventions, definitions and obligations of confidential relationships, and enforceability of non-compete agreements. If the concern is preservation of evidence and enforceability of judgments, the US already has a rich body of law and procedure that solves most of these problems, including the diversity jurisdiction of federal courts, multi-district litigation procedures, cross-border discovery procedures, and cross-border enforcement procedures. Additionally, it is worth noting that the Acts cannot and do not address the significant systemic challenges associated with getting jurisdiction over and enforcing judgments against foreign entities, infirmities which, standing alone, should cause Congress to pause.

The Acts' seizure provisions require special attention. The DTSA's provisions that would authorize motions to preserve evidence and seize property are not necessary in light of the broad discretion that federal courts already have under the Federal Rules of Civil Procedure⁸ to grant temporary restraining orders *ex parte* and would arguably

⁶ U.S. CONST., Art. I, § 8, cl. 3.

⁷ See *The Trademark Cases*, 100 U.S. 82 (1879) (Congress has limited powers to legislate under the Commerce Clause).

⁸ See FRCP 65 (2014).

interfere with the Rules Enabling Act process.⁹ Moreover, litigants can already request preliminary relief in trade secret cases and there are severe consequences for the destruction of evidence under existing law and rules of professional conduct.

Similarly, the TSPA's provision, while not as broad as the DTSA's, acknowledges but fails to ameliorate the problems and risks associated with seizure. First, the TSPA specifies that such relief is only available upon a showing that the preliminary relief that is available under FRCP Rule 65(b) is inadequate, a threshold that we believe will be difficult to establish, thereby making the provision superfluous. Second, the required showing is nearly identical to the standards that federal courts currently apply when deciding whether to grant preliminary relief, but with the odd additional requirement that "the applicant has not publicized the requested seizure." The purpose of this requirement and the provision requiring "protection from publicity" is unclear, but we are concerned that the TSPA requires a level of secrecy about court rulings that is unprecedented. The required procedures and findings are also bound to impose great burdens on the federal courts, and like the problems with the jurisdictional clause discussed above, arguably put trade secrets at greater risk. Of even greater concern (for reasons that are explained below), we are concerned about the anti-competitive effects of the seizure remedy.

Therefore, the Acts will exacerbate rather than solve the perceived problem of a lack of uniform state law, with no corresponding benefits and several significant drawbacks.

3. The Acts are imbalanced and could be used for anti-competitive purposes.

A hallmark of all US intellectual property laws, including trade secret law, is that they include limiting doctrines that are designed to achieve the appropriate balance between the protection of intellectual property rights and the preservation of free competition. While the Acts appropriately define "improper means" not to include the acts of reverse engineering and independent derivation, other limits on the scope of trade secret protection are missing. In particular, we note that the Acts do not explicitly limit the length of injunctive relief to the period of lead-time advantage, a critical limit on potentially interminable injunctions that can prevent fair competition, employee mobility and new innovation. Additionally, the seizure provisions of both Acts, but

⁹ See 28 U.S.C. § 2072 (2014).

particularly of the DTSA, introduce a new form of preliminary relief that is fraught with potential misuse due to the fact that such relief could be granted *ex parte*, without either notice to or an opportunity to be heard by the defendant(s). Both of these failures could render the Acts a weapon of anti-competition and societal damage with, again, no corresponding benefits.

4. The Acts increase the risk of accidental disclosure of trade secrets.

Because of the jurisdictional issue discussed in Point Two, there will likely be many motions to dismiss for lack of subject matter jurisdiction that, as a practical matter, will require the plaintiff to identify and disclose its trade secrets early in the litigation. But under all existing US trade secret law, the understandable common plaintiff strategy is to delay the identification and disclosure of trade secrets until the latest possible moment due to the heightened disclosure risk that comes from even the confidential sharing of information. Thus, if the existence and nature of the alleged trade secrets are necessary to establish jurisdiction under the Acts, defendants in trade secret cases will be justified in demanding earlier disclosure of the alleged trade secrets. This will result in a greater risk of accidental disclosure of the trade secrets and slow down the litigation process, with, again, no corresponding benefits.

5. The Acts have potential ancillary negative impacts on access to information, collaboration among businesses and mobility of labor.

While the Acts appear to be ineffective and/or unnecessary in combatting actual cyber-espionage and other misappropriation, they may have more impact on the negative side of the equation, namely, as an additional weapon to prevent public and regulatory access to information, collaboration amongst businesses, and mobility of labor. Although not often linked, there is a direct relationship between availability of trade secret misappropriation claims and regulatory access to information. Labeling information as a trade secret has become a common way to prevent public and even regulatory access to important information ranging from the composition of hydraulic fracturing fluids to the code inside of voting machines, all of which have compelling (but not uncontroversial) reasons for public access in a democracy. These access to information issues – which do not necessarily correlate with support for or opposition to the subject activities or industries – are exacerbated even by otherwise ineffective trade secret law.

The threat of a trade secret misappropriation action can and does have a chilling effect on collaborative innovation efforts between businesses and can be used by those who would rather compete in a courtroom than the marketplace to quell legitimate competition. Adding a new remedy that allows companies to seek preliminary relief to seize wide swaths of property (including computer networks and servers) would only heighten the risk that trade secret litigation will be used as an anti-competitive tool.¹⁰

Lastly, the importance of employee mobility to the strength and growth of our economy cannot be overstated. Reducing mobility of labor impacts not only those employees who are directly affected, but their new employers and the families of the affected employees. It also has an adverse impact on society by reducing the diffusion of skills and knowledge and stifling the innovation that flows from the sharing of ideas and information. State law currently protects employee mobility; the Acts do not.

If Congress is going to further strengthen arguments against access to information and simultaneously further limit mobility of labor and potential innovative collaboration, as adding yet another potential (even if ineffectual) trade secret misappropriation cause of action to the books would do, it should be because the benefits of such a cause of action outweigh the costs. Here, as previously discussed, the benefits are nonexistent. Therefore, the ancillary costs are not nearly outweighed; in fact, the scale leans decidedly to one side.

In sum, Congress is rightly concerned about cyber-espionage by foreign countries and foreign business interests, but adding to well-established domestic trade secret law to address such concerns is incomplete, ill-advised, and potentially dangerous. The Acts are incomplete solutions because the definition of a trade secret

¹⁰ The Acts' seizure provisions are eerily similar to the problematic provisions in copyright law's failed Stop Online Piracy Act ("SOPA") and Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act ("PIPA"). SOPA and PIPA were intended to combat online copyright infringement, but were never passed in large part because of problematic provisions related to removal of allegedly infringing websites from the Internet. See Mark Lemley, David S. Levine and David Post, *Don't Break the Internet*, 64 STAN. L. REV. ONLINE 34 (Dec. 19, 2011) ("Websites can be 'completely removed from circulation'—rendered unreachable by, and invisible to, Internet users in the United States and abroad—immediately upon application by the government, without *any* reasonable opportunity for the owner or operator of the website in question to be heard or to present evidence on his or her own behalf. This falls far short of what the Constitution requires before speech can be eliminated from public circulation") (emphasis in original).

under US (and international law) is limited and does not protect all of the information that may be the subject of cyber-espionage, or even all of the information that many businesses believe are trade secrets. The Acts are ill-advised because they focus on trade secret misappropriation instead of the bad acts of cyber-espionage and foreign espionage – *which is where Congress should focus its legislative efforts*.¹¹ Finally, the Acts are dangerous because the many downsides explained above have no – not one – corresponding upside.

Thus, for all of the above reasons, we oppose the Acts and urge their rejection. Additionally, if not withdrawn, we ask Congress to schedule full hearings so that our views, and all others, can be fleshed out, challenged and discussed in an open forum. The important issues that you are trying to address require and deserve more deliberation and input. While we recognize that there have already been some hearings, the specific language of the Acts, their effectiveness and their ramifications must be discussed and debated in public hearings.

With regard to this letter, you may address any reply or correspondence to its authors and organizers, Professor David S. Levine (dsl2@princeton.edu) and Professor Sharon K. Sandeen (ssandeen@hamline.edu).

Signed,¹²

Professor Brook K. Baker
Northeastern University School of Law

Professor Mario Biagioli
UC Davis School of Law

Professor Barbara B. Bressler
DePaul University College of Law

¹¹ See, e.g., Sharon K. Sandeen, *The Third Party Problem: Assessing the Protection of Information through Tort Law*, in INTELLECTUAL PROPERTY PROTECTION OF FACT-BASED WORKS (Robert F. Brauneis, ed., 2009) (discussing ways to combat bad acts that do not depend on the IP status of the underlying information).

¹² All institutions are listed for identification purposes only and the signatories do not speak for or on behalf of their respective institutions.

Professor Irene Calboli
Marquette University Law School

Professor Michael A. Carrier
Rutgers Law School

Professor Brian W. Carver
University of California, Berkeley
School of Information

Professor Eric R. Claeys
George Mason University School of Law

Professor Thomas F. Cotter
University of Minnesota Law School

Professor Eric Fink
Elon University School of Law

Professor Shubha Ghosh
University of Wisconsin, Madison, School of Law

Professor Eric Goldman
Santa Clara University School of Law

Professor Robert A. Heverly
Albany Law School of Union University

Camilla Hrdy
Fellow
Center for Technology, Innovation and Competition
University of Pennsylvania Law School

Professor Peter Jaszi
American University Law School

Professor Lawrence Lessig
Harvard Law School

Professor David S. Levine
Elon University School of Law
Visiting Research Collaborator
Center for Information Technology Policy
Princeton University

Professor Yvette Joy Liebesman
Saint Louis University School of Law

Professor Brian J. Love
Santa Clara University School of Law

Professor Joseph Scott Miller
University of Georgia School of Law

William J. Moner
Instructor of Communications and Interactive Media
Elon University School of Communications

Professor Ira Steven Nathenson
St. Thomas University School of Law

Professor Phillip Edward Page
South Texas College of Law

Professor Frank Pasquale
University of Maryland School of Law

Professor Michael Risch
Villanova University School of Law

Professor Elizabeth Rowe
University of Florida Levin College of Law

Professor Pamela Samuelson
University of California, Berkeley School of Law

Professor Sharon K. Sandeen
Hamline University School of Law

Professor Kurt Saunders
California State University, Northridge
David Nazarian College of Business and Economics

Professor Christopher Seaman
Washington and Lee University School of Law

Professor Katherine J. Strandburg
New York University School of Law

Professor Tim Wu
Columbia Law School

CHAIR

Theodore H. Davis, Jr.
Atlanta, GA

CHAIR-ELECT

Donna P. Suchy
Cedar Rapids, IA

VICE-CHAIR

Scott F. Partridge
Houston, TX

SECRETARY

Susan M. McGahan
Bedminister, NY

FINANCIAL OFFICER

Kim R. Jessum
Philadelphia, PA

CLE OFFICER

Jonathan Hudis
Washington, DC

MEMBERSHIP OFFICER

George W. Jordan III
Houston, TX

**SECTION DELEGATES TO
THE HOUSE OF DELEGATES**

Susan B. Montgomery (2016)
Boston, MA

Joseph M. Potenza (2017)
Washington, DC

William L. LaFuze (2018)
Houston, TX

IMMEDIATE PAST CHAIR

Lisa A. Dunner
Washington, DC

COUNCIL MEMBERS

L. Marisa Campbell (2016)

Dale Cendali (2016)

Willard Jones (2016)

Adriana S. Luedke (2016)

Steven P. Caltrider (2017)

Herbert D. Hart III (2017)

Patricia S. Smart (2017)

Mark Whitaker (2017)

Thad Chalomentiarana (2018)

Nancy M. Lambert (2018)

Janet Hendrickson (2018)

Darrell G. Mottley (2018)

Scott M. Alter (2019)

Janet Fries (2019)

Barbara J. Gislason (2019)

Heath W. Hoglund (2019)

Young Lawyer Council Member

Sharra S. Brockman (2016)

SECTION STAFF

Michael G. Winkler
Director

Carey Farley
Programming / Events

Amy Mandel
Communications / Publications

AMERICAN BAR ASSOCIATION

October 5, 2015

Honorable Charles E. Grassley
Chairman
Committee on the Judiciary
United States Senate
Washington DC, 20510

Honorable Patrick J. Leahy
Ranking Member
Committee on the Judiciary
United States Senate
Washington DC, 20510

Section of Intellectual Property Law

321 North Clark Street

Chicago, IL 60654-7598

(312) 988-6254

FAX: (312) 988-6800

E-mail: iplaw@americanbar.org

www.americanbar.org/iplaw

Re: S. 1890, the Defend Trade Secrets Act of 2015

Dear Chairman Grassley and Ranking Member Leahy:

I write to express the views of the American Bar Association Section of Intellectual Property Law on S. 1890, the "Defend Trade Secrets Act of 2015." These views have not been submitted to or approved by the ABA House of Delegates or Board of Governors, and should not be considered to be views of the Association.

There is no generally applicable federal private cause of action whereby an owner of a trade secret can seek redress for misappropriation of a trade secret. Relief must be sought under state law, and most states and the District of Columbia have in effect some version of the Uniform Trade Secrets Act (UTSA).

Congress recognized the need for federal protection of trade secrets when it enacted the Economic Espionage Act of 1996. That law authorizes criminal penalties of imprisonment for up to 15 years and a fine of not more than \$10,000,000 for the theft of trade secrets for the benefit of a foreign government or other foreign interest. Lesser penalties are provided for misappropriation not benefiting foreign interests but which relate to products in interstate or foreign commerce. The Attorney General of the United States has the authority to seek injunctive relief against the theft of trade secrets, but the Act does not contemplate a private cause of action by the owners of those trade secrets. The Section of Intellectual Property Law supports establishment of such a cause of action, and urges the enactment of S. 1890 for this purpose.

Currently in the United States, trade secrets are protected under an un-harmonized patchwork of trade secret laws that is ill-equipped to provide an effective civil remedy for companies whose trade secrets are stolen. Not all states have adopted the UTSA, and many differ in the interpretation and implementation of existing laws. For instance, many states define protectable trade secrets differently and also have different requirements for the maintenance of claims for trade secret misappropriation. To give but two examples, some states have found a novelty requirement for information to be considered a trade secret, and some are more protective than others of customer lists.

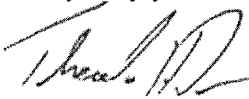
States have differing statutes of limitations for trade secret claims, and there are also significant differences in the availability of monetary relief. Many states have not enacted Section 8 of the UTSA, which calls upon each state to construe and apply the law to achieve uniformity among states. Moreover, victims of trade secret theft can face lengthy and costly procedural obstacles in obtaining evidence when the misappropriator flees to another state or country or transfers evidence outside the state.

S. 1890 is the product of several years of congressional consideration and development. The Section of Intellectual Property Law has followed these developments and, in doing so, has identified essential components that should be included in a bill to establish a federal private cause of action for misappropriation of a trade secret. These components include:

- a definition of trade secret that is clear and effective and not unduly restrictive or overly technical;
- a clear delineation of the requirements for a federal cause of action;
- the availability of remedies that are comparable to those available under the UTSA, including provisions providing for injunctive relief and monetary relief in the form of royalties, disgorgement of the proceeds of unjust enrichment, and exemplary damages;
- provisions for seizure orders that adequately limit the circumstances in which they may be issued and executed and that provide for the custody, security, and access to seized property; and
- confirmation that the bill's enactment will not preempt state trade secret laws.

Because S. 1890 contains these essential components, the Section of Intellectual Property Law supports its enactment.

Very truly yours,



Theodore H. Davis Jr.
Section Chair
American Bar Association
Section of Intellectual Property Law

December 1, 2015

The Honorable Charles E. Grassley
Chairman
Committee on the Judiciary
United States Senate
224 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Patrick J. Leahy
Ranking Member
Committee on the Judiciary
United States Senate
152 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Orrin G. Hatch
Committee on the Judiciary
United States Senate
104 Hart Senate Office Building
Washington, DC 20510

The Honorable Christopher A. Coons
Committee on the Judiciary
United States Senate
127A Russell Senate Office Building
Washington, DC 20510

Re: AIPLA Support for S. 1890, the Defend Trade Secrets Act of 2015

Dear Chairman Grassley, Ranking Member Leahy, Senator Hatch and Senator Coons:

I am writing on behalf of the American Intellectual Property Law Association (“AIPLA”) to express our support for S.1890, the Defend Trade Secrets Act of 2015, which would amend the Economic Espionage Act of 1996 (“EEA”) to create a federal civil remedy for trade secret misappropriation.

AIPLA is a national bar association of approximately 14,000 members who are primarily lawyers engaged in private or corporate practice, in government service, and in the academic community. AIPLA members represent a wide and diverse spectrum of individuals, companies, and institutions involved directly or indirectly in the practice of patent, trademark, copyright, trade secret, and unfair competition law, as well as other fields of law affecting intellectual property. Our members represent both owners and users of intellectual property. Our mission includes helping establish and maintain fair and effective laws and policies that stimulate and reward invention while balancing the public’s interest in healthy competition, reasonable costs, and basic fairness.

The economy of the United States depends on the innovations of its businesses. There has been a significant increase in commentary and media reports describing a growing rise in trade secret theft from foreign hackers, international companies, and rogue employees interested in stealing U.S. businesses’ trade secrets. In February 2013, President Obama’s Administration issued a

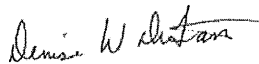
The Honorable Charles E. Grassley
The Honorable Patrick J. Leahy
The Honorable Orrin G. Hatch
The Honorable Christopher A. Coons
December 1, 2015
Page 2

report on the Strategy on Mitigating the Theft of Trade Secrets, which recognized the increasing problem of trade secret theft against U.S. corporations.¹

AIPLA believes that although state trade secret laws afford U.S. companies many protections, they may not provide adequate procedural remedies or protection in all cases of trade secret misappropriation. The ability to have a national approach and be able to utilize the broad jurisdictional powers of federal courts would greatly assist many trade secret claimants. Accordingly, AIPLA believes that a federal civil cause of action empowering companies to protect their own trade secrets from misappropriation, such as that which would be established by S. 1890, is imperative. Despite their best efforts, government agencies and prosecutors may not be able to move as quickly or with the nimbleness of a private litigant in some circumstances. Given the importance of speed and injunctive relief in many trade secret cases, a federal private right of action would be a powerful tool in the case of trade secret misappropriation.

AIPLA appreciates the Committee's attention to this issue. We believe that the time has come for a federal civil remedy for trade secret misappropriation, and we look forward to working with the Committee on S. 1890 as the process moves forward.

Sincerely,



Denise W. DeFranco
President
American Intellectual Property Law Association

¹ Executive Office of the President of the United States, Administration Strategy on Mitigating the Theft of U.S. Trade Secrets 1 (2013), https://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf.

CORPORATE COUNSEL

Time to Modernize and Strengthen Trade Secret Law

By Mark L. Krotoski and Greta L. Burkholder

December 1, 2015-The U.S. Senate Judiciary Committee has scheduled a hearing for Dec. 2 on a subject that is important to our national economy and security: protecting trade secrets. The hearing will highlight bipartisan legislation, the Defend Trade Secrets Act (DTSA), that, if enacted, will modernize and strengthen trade secret law and address a number of weaknesses under current law. The legislation has been introduced by Senators Orrin Hatch (R-UT) and Chris Coons (D-DE) and Representatives Doug Collins (R-GA) and Jerrold Nadler (D-NY).

The bipartisan support isn't surprising, even in the current Congress. After all, who is against protecting trade secrets? Trade secrets provide tremendous benefits to the national and local economies. They support, jobs, innovation and new products and services. Trade secrets--which can take many forms such as source code, formulas, secret recipes and prototypes--have many owners, from small businesses, startups, medium and large companies and individuals and groups who have yet to form a company.

Because of their significant value, however, they are often targeted for theft and misappropriation by insiders, competitors and more recently perpetrators of cyber espionage. Thieves can reap the benefit of potentially millions of dollars in prior research and development invested in trade secrets. The cumulative cost has been estimated to be from one to three percent of the Gross Domestic Product of the United States and other advanced industrial economies.

Unfortunately, under current law, obtaining a meaningful remedy can be costly, cumbersome and ineffective. Today, civil trade secret remedies are based solely on state, but not federal law. State trade secret laws provide an important remedy for local trade secret theft, however, in today's global economy, state laws are often ineffective in redressing theft of trade secrets that are removed to other jurisdictions. For example, obtaining a deposition of a witness in another state can require multiple court orders in different jurisdictions and lengthy delays.

In limited circumstances, federal courts may apply state trade secret law where jurisdiction is based on diversity of citizenship among the parties and the matter in controversy exceeds \$75,000 (known as diversity jurisdiction). However, diversity jurisdiction is not available where the parties are from the same state, even if the trade secret was removed to another state or outside the country. Under this jurisdiction, the federal court is applying state and not federal trade secret law.

What may be most troubling is that policies to encourage and promote trade secrets are undermined by an inability to obtain meaningful remedies. The most important remedy, of course, is the ability to recover trade secrets after they are stolen. But these days trade secrets can readily be emailed or transferred to other jurisdictions within minutes or hours. DTSA advances a number of significant benefits. DTSA would, for the first time, afford trade secret owners the option of a federal private right of action for trade secret theft. Claims for the infringement of other forms of intellectual property, including copyrights,

trademarks, and patents, are heard in federal court. There is no reason why this same option should not be extended to trade secrets, which is one of four intellectual property rights. Trade secret owners would have a choice of seeking relief in either federal or state court where the jurisdictional requirements are met. This gives them more choices on the best forum for the case.

Second, DTSA provides an effective, reasonable and balanced means to recover stolen trade secrets. In any trade secret case, one of the highest priorities is to recover the stolen trade secrets. Regrettably, they rarely are. Current law lacks an effective mechanism to help make that possible. The legislation would provide a federal court the authority to issue a short-term, ex parte civil order, under limited circumstances and upon a sufficient showing, to seize allegedly stolen trade secrets and prevent their transfer. The ex parte provision simply allows the federal court to preserve the status quo pending a full hearing within seven days with all parties. This part of the legislation also contains a number of safeguards. For example, it requires that the seized material be brought within the custody of the court, and enables the court to consider any claims of abuse in the ex parte seizure.

Third, DTSA includes provisions that recognize the realities of trade secret theft in the digital era. For example, the court can "secure the seized material from physical and electronic access during the seizure and while in the custody of the court." A party can request that any seized materials be encrypted.

Fourth, by amending an existing statute, the Economic Espionage Act (EEA) of 1996, which is a criminal statute, DTSA would create new civil remedies and draw upon practice and experience with a statute that has been used effectively for criminal cases. For example, the federal protective order provision has been used successfully to safeguard a wide variety of trade secrets and is stronger than state law. The definition of a trade secret is broader than the definition under the UTSA as it is more descriptive in its coverage and expressly applies to intangible information.

Fifth, the legislation would establish a five year statute of limitations, which is longer than the three year statute under the Uniform Trade Secrets Act (UTSA), which has been adopted by 47 states. Trade secret theft cases can be challenging and difficult to investigate and prove. Often the time to establish and understand the full scope of the misappropriation and the nature and circumstances may take a substantial amount of time. Finally, the legislation strengthens the options for remedying trade secret theft by providing trade secret owners with a choice of federal or state law. The legislation explicitly does not preempt state trade secret laws, which means that trade secret owners will continue to have a choice.

Some questions about the legislation have been raised. In considering the answers to these questions, the benefits of the legislation are reinforced.

Could DTSA increase litigation and other costs for trade secret cases? Actually, DTSA would reduce costs in a number of key respects. If the ex parte seizure order results in the recovery of stolen trade secrets, the cost savings will be tremendous. The inability to recover the stolen trade secrets in state court means the trade secrets may be used by others. The thief obtains a windfall by benefitting from the prior research and development invested in the trade secrets.

DTSA will promote litigation costs savings. The costs of litigation will often turn on the facts of the case. A local misappropriation may be well-suited for state court resolution. However, the state court process is cumbersome and more costly when the trade secret has

been taken to other jurisdictions. Under the legislation, the costs of litigation will be lower as a federal court can order discovery and depositions, and enforce a judgment more efficiently and effectively than state courts.

Will the new seizure order provision place small companies at a disadvantage?

Actually, small companies, start-ups and individual trade secret owners may benefit from the ability to use the new seizure provision. Often trade secrets are first developed in a small organization. A small company may benefit from its ability to use the ex parte seizure provision to recover them through the federal court.

Are the reforms too strong? Are they likely to promote wrongful claims? In the event of any abuse of the seizure provision, the legislation contains a number of safeguards. In order to obtain a court-ordered seizure, the applicant must describe the trade secret with sufficient particularity in order to allow the court to evaluate the request. The provision contains restrictions about the publicity of the seizure, in order to protect those who might be unfairly targeted. And, among other protections, the legislation would also create a private right of action for a person who suffers damage by a wrongful or excess seizure. The court can also award “reasonable attorney’s fees to the prevailing party” for “claims of misappropriation made in bad faith.”

Will the federal legislation “de-harmonize” state trade secrets law? Actually, the federal legislation strengthens and modernizes trade secret law to address the technological realities and other challenges of today. The current federal criminal statute, the Economic Espionage Act of 1996, was originally based in large part on UTSA, which was last amended in 1985. Many states have adopted variations to the UTSA model. The problem is that UTSA is now outdated in many respects. A more-than-30-years-old statute model statute has failed to keep up with the technological advances and other challenges confronting trade secret law today particularly in our global and national. The new legislation builds upon the UTSA framework to modernize and strengthen trade secret law.

Is there any risk of “trade secret trolls”? So-called “trade secret trolls” are a legal fiction and have never been seen over the past few decades under UTSA. The claim is that the problem of “patent trolls” (in which a patent owner does not use the patent to develop products but brings patent infringement suits) may arise for trade secrets. Trade secrets differ from patents in key ways. Trade secret misappropriation requires access to the specific trade secret and misappropriation by improper means or unauthorized acquisition. There is no reason to believe that “trade secret trolls” could ever arise.

In conclusion, the bipartisan DTSA, which is supported by many businesses, makes long overdue advances to strengthen and modernize trade secret law. DTSA would amend current law in a fair and measured way and by allowing for more meaningful remedies and enabling a court to address any abuses. Given the importance of trade secrets to national and economic security, innovation, jobs, and growth, Congress should enact this bipartisan legislation.

Mark Krotoski is a partner in the litigation, privacy and cybersecurity, and antitrust practice groups of Morgan, Lewis & Bockius, in the Silicon Valley office. He previously served as the national coordinator of the Computer Hacking and Intellectual Property (CHIP) program in the Criminal Division of the U.S. Department of Justice, and as a CHIP prosecutor in Silicon Valley, where he prosecuted a range of computer intrusions, computer crimes and trade secret cases. Greta Burkholder is an associate in the firm’s antitrust practice group. She focuses on mergers and acquisitions, cartel investigations and civil and criminal antitrust

litigation. The views of the authors do not necessarily represent those of the firm or its clients.

Link to article on Corporatecounsel.com:

<http://www.corpcounsel.com/id=1202743712802/Time-to-Modernize-and-Strengthen-Trade-Secret-Law?kw=Time%20to%20Modernize%20and%20Strengthen%20Trade%20Secret%20Law&n=20151201&pt=Afternoon%20Update&src=EMC-Email&et=editorial&bu=Corporate%20Counsel>

Reprinted with permission from the December 1, 2015 edition of Corporate Counsel© 2015 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. ALMReprints.com – 877-257-3382 - reprints@alm.com.



November 30, 2015

The Honorable Charles E. Grassley
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

The Honorable Patrick J. Leahy
Ranking Member
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Chairman Grassley and Ranking Member Leahy:

I am writing to express our strong support for S. 1890, the Defend Trade Secrets Act of 2015. IPO is a trade association representing companies and individuals in all industries and fields of technology who own, or are interested in, intellectual property rights. IPO's membership includes almost 300 companies and more than 12,000 individuals who are involved in the association through corporate and other classes of membership.

The current legal tools available to remedy trade secret theft are inefficient and inconsistent with other areas of intellectual property law. The current federal law in this area has limitations. Though the FBI and Department of Justice do a good job enforcing the Economic Espionage Act, they have limited resources and numerous priorities and are not able to pursue all trade secret thefts. Likewise, state trade secret laws are not well-suited to respond to the movement of trade secrets across state and international borders or to act swiftly to preserve evidence and protect trade secrets from being further divulged. S. 1890 will create a federal remedy that will provide a uniform legal framework for our members and others to protect their trade secrets.

Creating a federal civil remedy is also important to our members' global competitiveness. International markets are affected by how countries protect intellectual property. Enacting this legislation will place the United States in a position to promote strong trade secrets protection globally, both by creating the "gold standard" by which countries can model their trade secrets laws and by placing the United States in a better position to negotiate trade agreements and other international treaties that provide strong trade secrets protection. America is a leader in innovation stimulated by strong intellectual property rights. S. 1890 is a vehicle for the United States to further that leadership by better protecting trade secrets.

Thank you again for your attention to this important issue.

Sincerely,

Mark W. Lauroesch
Executive Director

cc: Senate Judiciary Committee

1501 M Street, NW, Suite 1150 • Washington, DC 20005
T: 202-507-4500 • F: 202-507-4501 • E: info@ipo.org • W: www.ipo.org

President
Philip S. Johnson
Johnson & Johnson

Vice President
Carl B. Horton
General Electric Co.

Treasurer
Kevin H. Rhodes
3M Innovative Properties Co.

Directors
Steven Arnold
Micron Technology, Inc.
Paul Bartusiak
Motorola Solutions, Inc.
Edward Blocker
Koninklijke Philips N.V.
Tina M. Chappell
Intel Corp.
Karen Cochran
DuPont
John Conway
Sanofi
William J. Coughlin
Ford Global Technologies LLC
Anthony DiBartolomeo
SAP AG
Luke R. Dohmen
Boston Scientific Corp.
Daniel Enebo
Cargill, Inc.
Barbara A. Fisher
Lockheed Martin
Louis Foreman
Enventys
Scott M. Frank
AT&T
David A. Frey
Rolls-Royce Corp.
Darryl P. Frickey
Dow Chemical Co.
Gary C. Ganzl
Evoqua Water
Technologies LLC
Krish Gupta
EMC Corporation
Henry Hadad
Bristol-Myers Squibb Co.
Michael Jaro
Medtronic, Inc.
Thomas R. Kingsbury
Bridgestone Americas
Holding Co.
Charles M. Kinzig
GlaxoSmithKline
David J. Koris
Shell International B.V.
William Krovatn
Merck & Co., Inc.
Dan Lang
Cisco Systems, Inc.
Allen Lo
Google Inc.
Timothy Loomis
Qualcomm, Inc.
Thomas P. McBride
Monsanto Co.
Steven W. Miller
Procter & Gamble Co.
Micky Minhas
Microsoft Corp.
Douglas K. Norman
Eli Lilly and Co.
Salvatore Pace
Praxair, Inc.
Richard F. Phillips
Exxon Mobil Corp.
Dana Rao
Adobe Systems Inc.
Curtis Rose
Hewlett-Packard Enterprise
Matthew Sarboraria
Oracle Corp.
Manny Schecter
IBM, Corp.
Steven Shapiro
Pitney Bowes Inc.
Dennis C. Skarvan
Caterpillar Inc.
Daniel J. Staudt
Siemens Corp.
Brian K. Stierwalt
ConocoPhillips
Brian R. Suffredini
United Technologies, Corp.
James J. Trussell
BP America, Inc.
Phyllis Turner-Brim
Intellectual Ventures, LLC
Roy Waldron
Pfizer, Inc.
BJ Watrous
Apple Inc.
Stuart Watt
Amgen, Inc.
Mike Young
Roche Inc.

General Counsel
Michael D. Nolan
Milbank Tweed

Executive Director
Mark W. Lauroesch

Statement of

Mark L. Krotoski

Submitted to the

U.S. Senate Judiciary Committee

For the Hearing on

“Protecting Trade Secrets:

The Impact of Trade Secret Theft on American Competitiveness

and Potential Solutions to Remedy This Harm”

December 2, 2015

Chairman Grassley, Ranking Member Leahy, and Members of the Committee, thank you for focusing on the important issue concerning the protection of trade secrets which impacts national and economic security matters. I appreciate the opportunity to submit this statement and I remain available to assist on any issues or questions that may arise.

I am a partner in the law firm of Morgan, Lewis & Bockius LLP in Silicon Valley, California, and in Washington, D.C. My practice focuses on assisting clients on trade secret, economic espionage, cybersecurity, and antitrust cartel enforcement cases and issues.¹

For nearly 20 years, I was privileged to serve as a federal prosecutor in the U.S. Department of Justice (DOJ) including leadership positions in the U.S. Attorney's Office for the Northern California and in the Criminal and Antitrust Divisions of the U.S. Department of Justice in Washington, D.C. Since first starting as a Computer Hacking and Intellectual Property (CHIP) prosecutor in the late 1990s, I had the chance to prosecute nearly every type of computer intrusion, computer crime, and intellectual property offense.

In Silicon Valley as a CHIP prosecutor, and later for nearly four years as the National Coordinator of the CHIP Program,² I focused on prosecuting foreign economic espionage and trade secret cases and serving as a DOJ leader on litigation and investigative issues under the Economic Espionage Act of 1996 (EEA).³ Of the eleven foreign economic espionage cases that have been authorized by the DOJ since 1996,⁴ I was fortunate to be involved in the successful prosecution of two of those cases. Both cases involved the misappropriation of trade secrets with the intent to benefit the government of the People's Republic of China (PRC). *See* Appendix A (summarizing the eleven foreign economic espionage cases during 1996 through 2015).

The first foreign economic espionage case that I participated in involved the misappropriation of a visual simulation software program trade secret used for training military fighter pilots and the export of a prohibited munitions list item that were brought to the PRC. The case was opened after a trade secret was displayed at a demonstration project at the PRC Naval Research Center in Beijing.⁵ Following an extensive investigation, defendant Xiaodong Sheldon Meng was charged with three Section 1831 foreign economic espionage counts involving multiple foreign government entities, including the Thai Air Force, Malaysian Air Force, and various PRC instrumentalities, and other counts.⁶ While preparing for a jury trial, defendant Meng ultimately pled guilty to two national security violations: committing foreign economic espionage with the intent to benefit the PRC Navy Research Center and violating the Arms Export Control Act and the International Traffic in Arms Regulations.⁷ The case was the second conviction and first sentencing for foreign economic espionage and the first conviction involving "source code" under the Arms Export Control Act.⁸

The second foreign economic espionage case I worked on involved the misappropriation of proprietary insecticide trade secrets and transfer of that information to the PRC and Germany for further development.⁹ I served as a member of the prosecution team with two other dedicated federal prosecutors and two FBI agents. The team successfully recovered some trade secrets in Germany through a Mutual Legal Assistance Treaty request for German law enforcement officials to obtain evidence.¹⁰ The investigation revealed that defendant Kexue Huang had traveled to the PRC as a part-time professor at Hunan Normal University, where he directed the

development of the misappropriated trade secrets. The PRC government had granted funding for further research.¹¹ Following an investigation, Huang was charged with twelve counts of foreign economic espionage and five counts of transportation of stolen property.¹² A few weeks before the scheduled trial, Huang pled guilty to one count of foreign economic espionage under Section 1831 involving Dow AgroSciences' trade secrets in the Southern District of Indiana, and to one count of the theft of Cargill's trade secrets under Section 1832 based on charges filed in the District of Minnesota.¹³ Huang was sentenced to 87 months in prison – the highest sentence for a negotiated plea agreement for foreign economic espionage to date.

Other trade secret cases I prosecuted involved cyber espionage of source code which was traced to a hacker outside the United States.¹⁴ I have also successfully handled more traditional trade secret cases.

Based on my experience gained when prosecuting these cases, I led the development of the DOJ's first training on economic espionage and trade secret cases for prosecutors and agents, and served as an instructor on cybersecurity and other law enforcement issues at the DOJ National Advocacy Center. I also served as the primary author to update the Theft of Commercial Trade Secrets chapter in the DOJ Prosecuting Intellectual Property Crimes Manual (Fourth Edition 2013).

Now in the private sector, I counsel clients on trade secret protection and cybersecurity measures, and represent them in trade secret cases. Given my background, I have firsthand experience in prosecuting foreign economic espionage and trade secret cases and in assisting trade secret owners in protecting their trade secrets. I have seen the intersection of criminal and civil cases and the challenges confronted under current law in obtaining adequate remedies under current state trade secret laws. Trade secret theft has also emerged as an important cybersecurity issue. Based on my practitioner's viewpoint, I have concluded that it is important for Congress to strengthen and modernize trade secret law to promote and protect trade secrets in the innovation process.

I. Overview

Because of the tremendous value of trade secrets in our economy, they remain a target for theft and misappropriation. State legislatures first addressed the problem of trade secret theft by enacting state trade secret laws. In 1979, the Uniform Trade Secret Act (UTSA) was first promoted, and then modified in 1985.¹⁵ Currently, 47 states have adopted some form of the UTSA. In 1996, Congress enacted the EEA to authorize federal criminal prosecution of foreign economic espionage and trade secret theft. The EEA was also largely premised on UTSA.

Many of the technological issues today were not contemplated when the trade secret statutes were first enacted decades ago. No one could conceive that in only a few minutes valuable trade secrets could be emailed or transmitted to other jurisdictions or outside the country. Issues about cyber espionage were not a major concern.

The time has come to modernize and strengthen trade secret laws to address the unique challenges of today. State civil trade secret laws should be reinforced with the option to use

strong and effective federal civil trade secret statute. Trade secret owners should have a choice on how best to obtain relief. For local trade secret theft, state laws can be effective. Once trade secrets are removed to other jurisdictions, and state laws may be less effective, trade secret owners should be able to rely on federal law to seek relief.

The bipartisan Defend Trade Secrets Act (DTSA) will modernize and strengthen trade secret law and resolve a number of deficiencies under current law. This statement reviews the role of trade secrets to innovation and our economy. The challenges under current law in obtaining meaningful remedies and the benefits of DTSA are noted. Finally, two suggestions are offered for consideration in addressing trade secret reform.

II. Significant Contributions of Trade Secrets to Innovation and the National Economy and Security

A. Many Products and Services in Many Industries

Trade secrets, as one form of intellectual property, serve a unique role in the innovation process and in our economy. Trade secrets can create new products, generate jobs, and lead to new consumer benefits and economic or technological advancements.

Trade secrets touch nearly every industry. Demonstrating the breadth of affected industries, recent cases have addressed trade secrets in industries such as agriculture, airplane parts, automobile, beverage, chemical, construction, executive recruiting, financial institution, fireworks, gas and oil, greeting cards, insurance, medical devices, paint, nutritional supplements, railroad, semiconductor manufacturing, toys, and wind turbine. *See* Appendix B (listing examples).

Trade secrets benefit companies of all sizes, including small businesses, and companies yet to be formed. The EEA has been successfully used to prosecute trade secret misappropriation for all types of businesses and organizations. Trade secrets may be developed by small companies that grow to be very large, which is consistent with the innovation process.

Trade secrets contribute tremendous value for consumers, their owners, employees, an industry and the economy. Consider, for example, the economic impact and many products generated by the Coca Cola formula trade secret or the Google search algorithm trade secret.

The benefits from trade secrets can be considered from macro and micro perspectives. At the macro level, trade secrets serve a fundamental role in advancing our national and economic security. One trade secret can help launch and generate numerous products or a new industry. On a micro level, trade secrets can foster economic growth for a company and generate jobs for its employees.

Trade secrets can take many forms and may include “financial, business, scientific, technical, economic, or engineering information” and can take many forms such as tangible or intangible plans, compilations, formulas, designs, prototypes, methods, techniques, processes, programs, and codes.¹⁶ Trade secret examples from recent civil and criminal cases show a

diverse range of trade secrets such as corn seed information; proprietary organic insecticides; brake pad specifications; Kevlar® technology used for body armor; fiber optic cables; high frequency trading strategy and infrastructure source code; information regarding gas and oil wells, including seismic data, geological maps, and reserves reports; information regarding the design and manufacturing of a disposable pen injector; an epoxy-based intumescent fireproofing material used in paint products; semiconductor manufacturing methods; designs of memory macros for computer chips; algorithm outlining how to implement a solution to compare different vehicles with different name features; design for computer memory chips; and wind turbine technology used to regulate the flow of electricity. *See* Appendix B (listing 35 trade secret examples from civil and criminal cases).

Trade secrets can also impact national security. In business, trade secrets provide a competitive advantage to their owners. When military application trade secrets are stolen, more than the loss of a competitive advantage is at risk. Instead, military or tactical advantages may be foregone. *See* Appendix C (listing examples).

B. The Costs from Trade Secret Theft

With the theft of a trade secret, the thief can reap the benefits of the investment in the trade secret, leap frog over generations of research and development, and destroy the competitive advantages maintained by the confidentiality of the trade secret. The cost of trade secret theft can be considered from both macro and micro perspectives.

On a macro level the cost of trade secret theft has been estimated to be “from one to three percent of the Gross Domestic Product (‘GDP’) of the United States and other advanced industrial economies.”¹⁷ The current U.S. GDP exceeds \$18 trillion.¹⁸

On a micro level, the theft of a single trade secret can adversely impact a company and jobs. Part of the trade secrets’ value is based on the investment of time and money in developing them. Many trade secrets represent the culmination of millions of dollars of investment and thousands of hours of research and development. In criminal cases, development costs have been considered as one measure of valuing loss from trade secret misappropriation.¹⁹

The true costs from trade secret theft remain difficult to measure adequately for a variety of reasons. The loss of the trade secret may be undiscovered for several years, and the loss as a result of the trade secret theft may be unknown or difficult to calculate. The scope of the trade secret loss may not be known. The loss may not be reported by the trade secret owner. Some trade secrets may lack valuation measures since they will launch new products and services.

A few recent civil and criminal individual cases provide examples on the value assigned to trade secrets in the litigation process:

- \$275 million loss estimated for the intended theft of trade secrets involving Kevlar® body armor technology from E.I. DuPont de Nemours & Co. with the intent to benefit the defendant company’s own product;²⁰

- \$40 million loss estimated for misappropriating hybrid motor technology from General Motors, with the intent to use said technology in a joint venture with an automotive competitor in China;²¹
- \$30.5 million awarded in damages by a jury for misappropriation of computer chip design memory macro trade secrets and breach of nondisclosure agreements;²²
- More than \$20 million loss estimated for misappropriating restricted technology and trade secrets related to the space shuttle program and Delta IV rocket;²³
- \$15.5 million loss estimated for the theft of more than 100 confidential chemical formulas used in the manufacture of silicone-based and rubber products;²⁴
- Stipulated value between \$7 million and \$20 million for misappropriating trade secrets involving proprietary organic insecticides from Dow AgroSciences with the intent to benefit the People's Republic of China and its foreign instrumentalities, and involving novel ingredients and process for a food product from Cargill;²⁵ and
- More than \$1.5 million loss for the theft of Coca-Cola trade secrets involving marketing information and product sample.²⁶

C. Forms of Trade Secret Theft and Misappropriation

Because of their tremendous value, trade secrets are the target of theft and cyber espionage. Trade secret owners confront both internal and external threats.

A common scenario involves an insider who has trusted access to valuable trade secrets and other confidential information and decides to steal them for his own benefit or for the benefit of others. The motives for this insider theft can vary. Some employees after years of service may become disgruntled. Some may be enticed to a new position with a competitor. Some may decide to start a new company using the stolen trade secrets and other information. Regardless of the circumstances, the trade secret owner is often surprised by the theft and typically feels betrayed.

An emerging area of concern involves cyber espionage. Recent developments confirm how these external cyber attacks present a serious threat to obtain trade secrets and other information. Cyber espionage may be directed by state actors or committed by hackers and organized groups focused on obtaining trade secrets and other information of value. A few cyber espionage examples are noted in reverse chronological order:

- On April 1, 2015, as part of an effort to develop new tools to address this problem, the White House issued an Executive Order declaring that cyber espionage has become a “national emergency.” The Executive Order authorizes the sanctions in appropriate cases against individuals and entities engaged in “malicious cyber-enabled activities,” including for “causing a significant misappropriation of ... trade secrets.”²⁷
- In December 2014, the FBI announced that it had attributed recent cyber attacks on Sony Pictures Entertainment to the North Korean government.²⁸ While this case did not involve trade secrets, it highlights the concerns raised by cyber espionage committed by state actors.

- In September 2014, an “international hacking ring” was indicted for stealing “trade secret data used in high-tech American products, ranging from software that trains U.S. soldiers to fly Apache helicopters to Xbox games that entertain millions around the world,” Assistant Attorney General Leslie Caldwell announced.²⁹
- In May 2014, five members of the Chinese military were charged with computer hacking, foreign economic espionage, and several other offenses in targeting six companies in the U.S. nuclear power, metals and solar products industries.³⁰
- In May 2009, in a case I prosecuted, a hacker from Sweden was indicted for hacking and copying source code of a leading network equipment provider and for hacking into National Aeronautics and Space Administration. Because there was no extradition treaty with the Kingdom of Sweden, the case was transferred for final prosecution to Sweden.³¹
- Other reports have traced state-sponsored hacking and the misappropriation of intellectual property to Chinese and Russian government groups.³²

III. Trade Secret Remedy Options Under Current Law

Since 1996, federal law only provides for the prosecution of criminal trade secret theft under the EEA. Consequently, the civil remedy for trade secret theft is based on local state laws.

Under current law, generally there are three avenues to seek remedies for trade secret theft:

- (A) Persuade the U.S. Department of Justice to investigate and prosecute a federal criminal case under the EEA;
- (B) File a civil case in state court; or
- (C) Try to establish federal jurisdiction based on either (a) diversity of citizenship jurisdiction relying on state legal theories, or (b) federal question jurisdiction by piggybacking the case onto another federal statute.

Each avenue presents challenges and limitations. On the first avenue, realistically, only a few trade secret cases qualify for federal criminal prosecution under the EEA. Not many trade secret cases are prosecuted by state prosecutors, and some penalties for state trade secret violations are relatively modest.

On the second course, state law may be effective at addressing local harms, but is less adept in redressing national or international theft of trade secret cases. Finally, efforts to stretch a trade secret case to satisfy current federal jurisdiction standards under other statutes often results in a poor fit for the case. These complications interfere with the ability for trade secret owners to obtain meaningful remedies under current law.

A. The Intersection of Criminal or Civil Remedies

As a federal prosecutor handling a variety of trade secret cases under the EEA, I was often asked to decide whether to open a trade secret case. I was able to see firsthand the intersection of criminal and civil trade secret remedies.

In deciding whether a trade secret case may be prosecuted as a criminal case under the EEA, prosecutors apply certain relevant “discretionary factors” under the U.S. Attorney’s Manual. These factors include:

- the scope of the criminal activity, including evidence of involvement by a foreign government, foreign agent or foreign instrumentality;
- the degree of economic injury to the trade secret owner;
- the type of trade secret misappropriated [i.e., did it involve sensitive technology or implicate national security];
- the effectiveness of available civil remedies;³³ and
- the potential deterrent value of the prosecution.³⁴

Other relevant factors may include:

- What was the manner of the misappropriation (e.g., criminal circumstances of theft, substantial planning and preparation for the misappropriation, or fraud)?
- Was the misappropriated trade secret used or what specific plans were made to use it?
- What steps were taken to disclose the trade secret to a foreign government or competitor?
- What evidence establishes the elements of the offense including criminal intent?
- What steps were taken for the trade secrets to leave the jurisdiction or country?

Under these factors, the U.S. Department of Justice has successfully prosecuted several significant foreign economic espionage and trade secret cases through the years.

As a practical matter, however, only a handful of trade secret theft cases will result in federal criminal prosecution. One key issue in all cases, including trade secret cases, is evidence to prove criminal intent. Even where the foregoing factors are met, the case may be declined for other reasons such as insufficient investigative resources. The criminal trade secret cases can be labor intensive depending on the circumstances. Some cases may take a few years to investigate and prosecute.

Apart from federal criminal prosecution, a few states have criminal statutes for the misappropriation of trade secrets. Some of the penalties, are generally modest.³⁵ The ability to bring state criminal trade secret cases is also a function of limited resources. State prosecutors are challenged when it comes to prosecuting international trade secret theft cases given limited resources and other limitations.

When trade secret cases were declined for criminal prosecution, the trade secret owner is left with civil remedies. On a number of occasions, the trade secret owners described their

concerns about whether they could obtain meaningful relief based on state law particularly for cases where the trade secrets were misappropriated to other states or outside the United States.

For me, these cases demonstrated the need for meaningful federal civil remedies to protect trade secrets. From my perspective, if the federal government declined criminal prosecution for appropriate reasons, policies to encourage intellectual property in the form of trade secrets are undermined if trade secret owners are unable to obtain effective relief.

B. Cumbersome and Costly State Law Process When Trade Secrets Are Transferred To Other Jurisdictions

State law may be useful for local misappropriation cases. As an example, if an employee steals an employer's trade secrets and brings them to a competitor across town or in another part of the same state, the same state judicial process and rules can be used to consider the misappropriation.

However, efforts to obtain remedies for the stolen trade secrets taken to other jurisdictions under state law can be cumbersome, costly and ineffective. Once trade secrets are stolen and removed to another state or outside the country, the legal options generally become more costly and complicated. The mere act of obtaining a deposition of a witness in another state can require multiple court orders and unacceptable delays.³⁶ Multiple court systems may also be necessary to subpoena records.

Instead, federal jurisdiction offers nationwide subpoena service power.³⁷ The ability to obtain one federal court order or issue one federal subpoena results in less delay and typically less cost than seeking the same or similar records or process through multiple state court systems. The cumbersome process and delays for interstate trade secret theft in state cases can serve as a significant disincentive to use an overburdened state court system.

C. Limited Options for Federal Court Jurisdiction

In order to seek relief, and avoid state court delays and challenges, trade secret owners may try to vindicate their rights in federal court. Although successful trade secret cases have been brought in federal court, obtaining federal jurisdiction is not always possible or a natural fit for the facts of the case. Current law provides two primary paths for federal court jurisdiction: (1) diversity jurisdiction or (2) federal question jurisdiction.³⁸

Diversity of Citizenship jurisdiction is available in limited circumstances where the "matter in controversy" exceeds \$75,000 and there is diversity of citizenship among the parties. This requires that the parties be from different states or involve a state citizen and non-citizen.³⁹ If diversity of citizenship is established, the federal court applies state law. This is the same state law that the state court would apply.

Diversity jurisdiction is not always available. It is nonexistent when the parties are from the same state even if the trade secret was removed to another state or outside the country. Even in those circumstances where diversity jurisdiction can be met, since the federal legislation

provides for greater protections of trade secrets than state law, trade secret owners will likely prefer the federal law. As noted in Section V(E), enhanced protections under the federal legislation include stronger protective order measures, a five-year statute of limitations, a broader definition of trade secrets, and an extraterritorial provision which applies to conduct outside the United States.

Where diversity jurisdiction is unavailable, trade secret owners may seek federal question (or subject matter) jurisdiction by using another federal statute.⁴⁰ In some cases, the Computer Fraud and Abuse Act (CFAA), may be an option.⁴¹ However, there are two significant restrictions. First, the CFAA does not apply where a computer was used and its other statutory requirements are not met. Second, even if a computer was used (for example to download or transfer the misappropriated trade secret), there is a significant circuit split on whether an insider or employee acting with the intent to steal the company's trade secrets and information with the company's computer violates the CFAA.⁴² Until this division among the courts is addressed, whether the CFAA may be used depends on which jurisdiction the misappropriation occurred.

Other federal statutes may be considered for federal question jurisdiction. However, the state trade secret claim would be considered under pendant or supplemental jurisdiction.⁴³ State law will still govern the trade secret misappropriation claim. The state trade secret claim may be weaker than the federal legislation, which fails to provide the most effective remedies and protection for trade secrets. Further, federal jurisdiction will be based on another statute (such as a trademark violation) that likely is not the primary basis for filing the case. Stretching the case as a means to enable jurisdiction often does not best fit the core facts of the case. The federal statute used for jurisdiction becomes the tail wagging the proverbial dog to obtain federal court review of the dispute. As with diversity jurisdiction, a federal trade secret statute, if enacted, would be preferable since it would provide more protections to trade secrets than current state law, as noted in Section V(E).

Consequently, because few trade secret cases rise to the level of a federal criminal prosecution, current law is dependent on state trade secret laws. Unless the trade secret theft is a local matter, state law is not effective to remedy trade secret theft in cases where the trade secrets are removed to other jurisdictions.

IV. Other Challenges in Obtaining Meaningful Remedies

Policies to encourage and promote trade secrets are undermined by an inability to obtain meaningful remedies resulting from the theft of trade secrets. When the entrepreneurial risks in time, effort, and money can be stolen without an effective remedy, innovation becomes stifled. The risks for innovation should be worth the unrealized reward.

There are a number of unique challenges in finding sufficient remedies for trade secret theft. In cases I have handled, certain challenges commonly arise in investigating and litigating trade secret theft cases. These challenges include:

- (1) The "misappropriation gap" advantage that a trade secret thief has in planning and stealing the trade secrets until the full scope of misappropriation is discovered;

- (2) The ease by which trade secrets can be transferred or transported to other jurisdictions in our global economy; and
- (3) The need to narrow the “recovery gap,” which is the time to recover the trade secrets after their misappropriation is discovered, and maintain the competitive advantage from the trade secrets for the owner and prevent their use and copying.

A. Overcoming the “Misappropriation Gap” Advantage During the Planning, Theft and Discovery Stages

Today trade secret thieves benefit from a “catch me if you can” environment. Under a risk-reward analysis, there is tremendous potential reward that can result from stealing trade secrets, measured against a lower risk of getting caught, recovery of the stolen trade secrets, and being held accountable in either a civil or criminal case. Recovery becomes more difficult in our legal system if the trade secrets are removed and transferred to other states or outside the United States. State law can be effective in addressing local misappropriation, but is less effective in dealing with the misappropriation of trade secrets to other jurisdictions or outside the United States.

Many trade secret cases involve what I have characterized in my cases as a “misappropriation gap.” This gap describes the time between the planning, preparation and actual theft of the trade secrets to the time of the discovery of the theft. The significance of this gap is that the trade secret thief maintains an advantage at this stage until full discovery of the theft. The reality is that it can take anywhere from a few months to a few years to learn about, investigate and uncover the full scope and manner of the misappropriation.

Significantly, the “misappropriation gap” advantage that the thief has often extends beyond the initial discovery. Often the full scope of the theft, including the number of stolen trade secrets, will not be known for a substantial amount of time.

The reality is that trade secret theft is often a highly reactive event for the trade secret owner.⁴⁴ The owner is usually surprised and caught off guard by the theft.

In trade secret cases, it is essential to uncover this “misappropriation gap” to learn about the scope of the trade secret theft. The sooner the misappropriation is discovered, the greater the chance to prevent loss of the trade secret including investments in research and development, and stop the use and copying of the trade secret.

Given the challenge of the “misappropriation gap,” based on my experience handling a variety of trade secret cases, the law needs to provide effective tools that promote the prompt seizure and recovery of trade secrets.

B. Ease of Misappropriating Trade Secrets to Other Jurisdictions

Today, our economy relies on information and technology in new ways that were unforeseeable when either the EEA was first enacted nearly 20 years ago, or the UTSA was adopted more than 35 years ago.

The ability to quickly transfer trade secrets to other jurisdictions has increased.⁴⁵ In today's global economy, within hours or a few days of the initial theft, the trade secret can be transferred or transported to other states or other countries. Once the secret is disclosed, the competitive value of the trade secret dissipates. The stolen trade secrets may never be recovered.

A common means to transfer and misappropriate trade secrets is by email. Consider a few case examples:

- After a defendant informed his employer “that he was going to remain with the company,” on the next day he “emailed a Microsoft Word document to his PKU [Peking University, College of Engineering, Department of Nanotechnology] email account which contained, embedded on the second page of an unrelated document, the protected chemical process.”⁴⁶
- Defendants were convicted for obtaining cell phone photographs of trade secret information and emailing the photographs to others.⁴⁷
- Trade secrets have been transmitted by email including to others outside the United States.⁴⁸

These are only a few examples but they demonstrate how quickly trade secrets can be removed from one jurisdiction and transmitted around the world. Given these challenges, the trade secret law should be modernized to address these electronic realities.

C. Narrowing the “Recovery Gap”

In addition to the “misappropriation gap,” which provides the trade secret thief with a substantial advantage until full discovery of the misappropriation, another important gap in these cases involves what is best described as the “recovery gap” which concerns the amount of time it may take to recover stolen trade secrets after discovery.

Time is certainly of the essence when it comes to recovering stolen trade secrets. Normally there is a small window of opportunity to recover stolen trade secrets. The best time to recover trade secrets is as close in time to the actual theft.

In each trade secret misappropriation case, one of the first requests and highest priorities of the trade secret owner is to recover the stolen trade secrets and prevent any copying or use. Often the stolen trade secrets can never be recovered. Current law lacks an effective mechanism to provide for the prompt trade secret recovery.

Any remedy that fails to address the “recovery gap” may fall short of meaningful relief. In criminal cases, search warrants can be used to seize trade secrets if their location can be identified. In civil cases, an appropriate mechanism with judicial oversight is needed to protect and recover trade secrets.

V. Modernizing and Strengthening Trade Secret Law and Establishing Effective Trade Secret Remedies

The bipartisan Defend Trade Secrets Act (DTSA) will modernize and strengthen trade secret law and resolve a number of deficiencies under current law. The legislation (S. 1890 and H.R. 3326) has been introduced by Senators Orrin Hatch (R-UT) and Chris Coons (D-DE) and Representatives Doug Collins (R-GA) and Jerrold Nadler (D-NY).

Based on the increasing importance of trade secrets to our economy, the legislation will help implement the original EEA objectives to promote national and economic security.⁴⁹ The legislation strengthens and modernizes trade secret law in a number of respects, noted below:

A. New Federal Private Right of Action

For the first time the legislation establishes a federal civil private right of action for trade secret misappropriation. Today, the only basis for a civil remedy of the misappropriation of trade secrets is under state and not federal law. While many states have adopted some version of UTSA, there are modifications and variations.

In limited circumstances, federal courts may apply state trade secret law where jurisdiction is based on diversity of citizenship, as noted in Section III(C). Under this jurisdiction, the federal court is applying state and not federal trade secret law. However, diversity jurisdiction is not available where the parties are from the same state, even if the trade secret has already been removed to another state or outside the country. DTSA would establish federal trade secret law. Under DTSA, trade secret owners would have a choice of seeking relief in either federal or state court where the jurisdictional requirements are met.

A federal private right of action will provide trade secret owners with meaningful remedies, particularly where trade secrets are removed from the original location and taken out of the state.

B. Filling a Gap in Federal Intellectual Property Law

The legislation fills a gap in current law by ensuring a federal private cause of action is available for all four intellectual property forms. Under current law, federal courts can hear claims of infringement in copyright,⁵⁰ trademark,⁵¹ and patent cases.⁵² However, civil trade secret misappropriation is based only on state law civil remedies.⁵³ Given the importance of trade secrets as intellectual property and to the role of innovation, there is no policy reason why trade secrets should not have similar federal protection. Federal law should encourage and promote the development of trade secrets just as it fosters other forms of intellectual property development.

Each type of intellectual property advances distinct objectives. Trade secret law protects information which provides a commercial advantage to its owner. Copyright law protects original creative works of authorship which may include computer software, motion pictures and sound recordings, and literary, musical, dramatic, choreographic, architectural, pictorial, graphic, and sculptural works.⁵⁴ Trademark law protects “any word, name, symbol, or device, or any

combination thereof” that identifies and distinguishes the source of goods.⁵⁵ Patent law protects inventions that are publicly filed and provides a “right to exclude others from making, using, offering for sale, or selling the invention throughout the United States or importing the invention into the United States.”⁵⁶

The different intellectual property forms can be interrelated. Trade secrets often serve as a precursor to patents. After initial development, the trade secret owner may decide to obtain protection under patent law by publicly filing the invention.

One trade secret may lead to other forms of intellectual property protection for related products. Consider for example the many products generated by the original Coca-Cola trade secret formula.⁵⁷ The words (“Coca-Cola”[®] and “Coke”[®]),⁵⁸ logo,⁵⁹ and bottle design have received trademark protection.⁶⁰ Design patents have also been issued on the bottle shape.⁶¹ Songs promoting the products, and advertising have copyright protection. These examples illustrate how one innovation can result in multiple forms of intellectual property protection.

Claims for the infringement of other forms of intellectual property, including copyrights, trademarks, and patents, are heard in federal court. There is no reason why this same option should not be extended to trade secrets as one of four intellectual property rights. National policy should encourage the development of all forms of intellectual property.

C. Reasonable, Balanced Mechanism to Recover Misappropriated Trade Secrets

The legislation addresses the “recovery gap” problem involving the need to promptly recover trade secrets and prevent any copying or use. The best time for recovery is as close in time to the theft. Prompt recovery minimizes the risk of unauthorized copying and use of the stolen trade secret.

Under the legislation, a federal court, under limited circumstances, can order the seizure of the trade secrets, bring them within the jurisdiction of the court, and hold a hearing to determine the appropriate response. The legislation is effective, reasonable and balanced in its approach and includes a number of safeguards to prevent potential abuse.

The legislation would provide a federal court the authority to issue a short-term, ex parte civil seizure order, upon a sufficient showing, to seize allegedly stolen trade secrets and prevent their transfer. A full hearing would be held within seven days with all parties. This part of the legislation contains a number of safeguards to balance the need for immediate action against the potential harm to a defendant.

The following six requirements ensure that the ex parte seizure order is limited to appropriate circumstances:

First, in seeking relief, the applicant must make a proper showing based on an affidavit or verified complaint.⁶² Specifically, the applicant must allege “specific facts” that demonstrate (1) a temporary restraining order under Rule 65 would be inadequate “because the party to which the

order would be issued would evade, avoid, or otherwise not comply with such an order;” (2) an “immediate and irreparable injury will occur” in the absence of seizure; (3) the harm in denying relief outweighs any harm to others; (4) the applicant is likely to succeed in showing the information is a trade secret and the person who is the subject of the order misappropriated or conspired to misappropriate the trade secret; (5) the matter to be seized is described with “reasonable particularity” and the location is identified; (6) the person subject to the order “would destroy, move, hide, or otherwise make such matter inaccessible to the court” if notice were provided; and (7) the requested seizure has not been publicized by the applicant.⁶³ Under this threshold step, no seizure order will issue absent a sufficient showing.

Second, in considering the application, the court must make certain findings and conclusions before issuing a seizure order. The seizure order shall (1) set forth findings of fact and conclusions of law required for the order; (2) provide for the “narrowest seizure of property” in a manner that minimizes any interruption of the business operations of third parties and, to the extent possible, does not interrupt the legitimate, unrelated business operations of the person accused of misappropriating the trade secret; (3) be accompanied by an order protecting the seized property from disclosure by restricting the access of the applicant and prohibiting any copies of the seized property; (4) set a prompt hearing within seven days after the order has issued; and (5) require the applicant to provide the security determined adequate by the court for payment of such damages as a person may be entitled to recover as a result of a wrongful or excessive seizure.⁶⁴ No seizure order will issue absent the required court findings are not made. Also, if the applicant cannot post the required security, the order will not issue.

Third, a neutral law enforcement official serves the seizure order and the “submissions of the applicant to obtain the order.”⁶⁵ This ensures that an experienced and unbiased professional executes the court’s order. By comparison, under current law a temporary restraining order may be served by an attorney or agent of a party, who may hold an interest in the outcome.

Fourth, any materials seized are retained into the custody of the court.⁶⁶ The court is required to secure the material from physical and electronic access.⁶⁷ Additionally, the court may take protective steps to verify that any electronic medium containing the trade secret is not “connected to an electronic network or the Internet without the consent of both parties, until the hearing” with all parties present. The seized material remains secure within federal court control.

Fifth, the court must hold a seizure hearing within seven days.⁶⁸ At the hearing, the court can consider the arguments from the parties. If the applicant is unable to meet its burden to establish sufficient facts to support the order, “the seizure order shall be dissolved or modified appropriately.”⁶⁹

Sixth, the legislation includes various safeguards against an improper ex parte seizure order. A motion to dissolve or modify the seizure order may be filed “at any time” by “any person harmed by the order.”⁷⁰ A person who suffers damage as a result of a wrongful or excessive seizure may bring a cause of action against the applicant to recover damages including punitive damages and a reasonable attorney’s fee.⁷¹ These statutory sanctions are in addition to general sanctions that the court may issue under Federal Rule of Civil Procedure 11.⁷² For any

claim of misappropriation that is made in bad faith, the court may award reasonable attorney's fees.⁷³

This balanced approach provides a new necessary tool to overcome the “misappropriation gap” and narrow the “recovery gap.” The provision increases the chances that trade secrets may be seized by a law enforcement official and maintained in the custody of the court pending a hearing involving all parties. The safeguards protect against potential abuse and provide the court with a variety of options to address any abuse. Because the recovery of trade secrets, particularly before any use or copying, may be the most important step following any misappropriation, the legislation enhances the chance for meaningful remedies.

D. Tools to Address Digital Era Issues

The legislation includes new provisions that recognize the realities of trade secret theft in the digital era. For example, the court can “secure the seized material from physical and electronic access during the seizure and while in the custody of the court.”⁷⁴ For information on an “electronic storage medium,” the court can protect the seized material by “prohibiting the medium from being connected to an electronic network or the Internet without the consent of both parties, until the hearing.”⁷⁵ A party can request that any seized materials be encrypted.⁷⁶

These provisions will help modernize trade secret law. Courts will be empowered to take appropriate steps to safeguard trade secrets during the litigation process.

E. Drawing Upon Meaningful Experience and Adopting Proven EEA Standards

Another benefit of the legislation is that it amends the current EEA statute by adding provisions for a civil remedy. In doing so, the legislation adopts and draws upon some of the stronger and effective standards that have been used in federal criminal cases. By amending the existing EEA, the legislation benefits from the practice and experience of a statute that has been used effectively for criminal cases. Some of these benefits include: (a) fostering employee mobility while prohibiting trade secret misappropriation; (2) using stronger standards to protect trade secrets during litigation; (3) using the broader definition of trade secrets covering intangible information; and (4) applying the extraterritorial provision.

A number of states which have adopted versions of the UTSA have also added criminal remedies as part of their trade secret laws.⁷⁷

1. Prohibiting Trade Secret Misappropriation While Fostering Employee Mobility

In amending the EEA to add the civil provisions, the legislation draws upon existing federal standards to promote employee mobility. For nearly 20 years the EEA has prohibited the misappropriation of a trade secret yet permitted the use of “general knowledge and skills developed while employed.”⁷⁸ In this manner, the EEA does not restrict employee movement; it only bars trade secret misappropriation.

During the House EEA debate 19 years ago, then-Representative Charles E. Schumer specifically addressed this issue:

[S]ome Members thought that this legislation might inhibit common and acceptable business practices. For example, employees who leave one company to work for another naturally take their general knowledge and experience with them and no one, no one wishes to see them penalized as a result.⁷⁹

During the Senate debate, Senator Herb Kohl also clarified:

[T]rade secrets are carefully defined so that the general knowledge and experience that a person gains from working at a job is not covered.

Mr. President, we do not want this law used to stifle the free flow of information or of people from job to job. But we built in a number of safeguards to prevent exactly these problems. They are elaborated on in the managers' statement and our committee reports.⁸⁰

The Managers' Statement further added:

This legislation does not in any way prohibit companies, manufacturers, or inventors from using their skills, knowledge and experience to solve a problem or invent a product that they know someone else is also working on. Thus, parallel development of a trade secret cannot and should not constitute a violation of this statute.

...

In addition, a prosecution under this statute must establish a particular piece of information that a person has stolen or misappropriated. It is not enough to say that a person has accumulated experience and knowledge during the course of his or her employ. Nor can a person be prosecuted on the basis of an assertion that he or she was merely exposed to a trade secret while employed. A prosecution that attempts to tie skill and experience to a particular trade secret should not succeed unless it can show that the particular material was stolen or misappropriated. Thus, the government cannot prosecute an individual for taking advantage of the general knowledge and skills or experience that he or she obtains or comes by during his tenure with a company. Allowing such prosecutions to go forward and allowing the risk of such charges to be brought would unduly endanger legitimate and desirable economic behavior.⁸¹

This distinction was further made in defining a trade secret:

In the course of reconciling the Senate and House versions of this legislation, we eliminated the portion of the definition of trade secret that indicated that general knowledge, skills and experience were not included in the meaning of that term. Its elimination from the statutory language does not mean that general knowledge can be a trade secret. Rather, we believed that the definition of trade secrets in itself cannot

include general knowledge. Thus, it was unnecessary and redundant to both define what does and what does not constitute a trade secret.⁸²

By amending the EEA, the legislation adopts and incorporates this line which bars trade secret misappropriation yet allows employees to use their general skill and knowledge.

2. Stronger Standards to Protect Trade Secrets During Litigation

Because the value and competitive advantages of a trade secret can be lost upon disclosure, it is essential to preserve the confidentiality of trade secrets during litigation. EEA Section 1835 contains effective standards to protect trade secrets during the litigation process. This provision has successfully safeguarded a wide variety of trade secrets and is stronger than comparable provisions under the UTSA or state law.

The UTSA recognizes that a court may issue a protective order.⁸³ However, the UTSA fails to address the situation in which a trial court orders the disclosure of trade secret information. This remains as an occasional risk during litigation process.

The EEA contains a stronger mechanism to safeguard trade secrets during litigation. EEA Section 1835 allows for an interlocutory appeal for review of an adverse disclosure ruling.⁸⁴ Without this statutory protection, an adverse ruling may not be appealable until after the conclusion of the entire case.⁸⁵ The legislation addresses this deficiency by using the stronger EEA protective order provision in civil cases.

Based on my experience prosecuting EEA cases, and in working closely with other prosecutors on EEA issues, the federal protective order provision has worked well to safeguard a wide variety of trade secrets. Since the EEA was enacted 19 years ago, only twice has an interlocutory appeal been sought under Section 1835. Both times the appellate court agreed with the government on the need to safeguard the trade secrets.⁸⁶ These cases demonstrate the importance of the shadow of potential and immediate appellate review. The legislation extends this protection to civil cases.

3. Broader Descriptive Definition of Trade Secrets Covering Intangible Information

The legislation uses the more descriptive and broader definition of trade secret information under the EEA.⁸⁷ In this manner, stronger protection is provided to trade secrets than under state law.

The trade secret definition under the EEA is based on the UTSA.⁸⁸ However, the EEA definition is broader than the UTSA in two areas. First, the federal definition is more descriptive in terms of what is covered. Second, the federal definition expressly applies to intangible information. In construing a statute, courts first consider the plain meaning of the statutory language to determine legislative intent.⁸⁹

Under the UTSA, a “trade secret” is defined as “information, including a formula, pattern, compilation, program, device, method, technique, or process.”⁹⁰ In contrast, the broader federal definition applies expressly to “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.”⁹¹ In 1996, Congress intended the federal definition to be broadly applied.⁹²

One of the objectives of the EEA was “to ensure that the theft of intangible information is prohibited in the same way that the theft of physical items is punished.”⁹³ Congress explicitly included intangible information in the definition of a trade secret. Consequently, the legislation provides stronger protection for trade secrets than under state law based on UTSA.

4. Extraterritorial Provision

In our global economy, many trade secrets are taken outside the United States. The EEA includes a specific extraterritorial provision which extends to the misappropriation of trade secrets outside the country.⁹⁴ By amending the current EEA, the legislation applies the extraterritorial provision to civil cases.

Because the UTSA does not include an extraterritorial provision, the general presumption against coverage of extraterritorial conduct applies in UTSA cases.⁹⁵ Federal law can best address this situation.

F. Longer Statute of Limitations

The legislation would establish a five year statute of limitations, which is longer than the three year statute of limitations under the UTSA⁹⁶ that is used by many states.

As noted, trade secret cases are often highly reactive. The period of the “misappropriation gap,” measuring the time of the planning and theft to discovery, can vary significantly. The trade secret owner may not discover the theft until the trade secret has been removed to another jurisdiction.

Even after discovery, the scope and nature of the misappropriation may remain unknown for some time. It is not uncommon for more trade secrets to have been stolen than initially realized. In some cases, it is not possible to determine how the trade secrets were stolen. The longer statute of limitations period recognizes these realities, provides a more realistic amount of time to seek relief, and increases opportunities to obtain meaningful relief.

G. Non-Preemption of State Remedies

The legislation does not preempt state law remedies. It therefore promotes remedies for trade secret theft by giving trade secret owners a choice to rely on either state or federal law as appropriate under the circumstances. The non-preemption also promotes greater deterrence

because trade secret owners can best decide whether relief is more appropriate in federal or state court. Trade secret thieves will risk the broader reach of federal law when trade secrets are removed to other jurisdictions. This approach is consistent with EEA Section 1838 which provides that the statute does not “preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret.”⁹⁷

Under our federal system, the dual option for state or federal remedies is common. For policy reasons, each jurisdiction may vindicate its interests. In other circumstances, federal and state law may overlap and reinforce common policies. For example, the Uniform Securities Act (USA) is used as a model for state securities law to cover “fraudulent activity ... at a level that eludes the applicability of federal law and, even when federal law applies, eludes the capacity of federal enforcement. Without state regulation accompanied by civil and criminal enforcement of the law in state courts, there would be no hope of redress for many victimized investors.”⁹⁸

As another example, a federal statute prohibiting age discrimination,⁹⁹ is supplemented by many state age discrimination statutes. Similarly, while most crimes are local, there is a benefit to allow prosecution of fraud at both the local and federal levels. As another example, many states have enacted laws prohibiting computer intrusions or unauthorized access to computers,¹⁰⁰ which supplements the Computer Fraud and Abuse Act which has both civil and criminal remedies.¹⁰¹

There may be a variety of reasons that a trade secret owner may select a federal or state forum. The owner may conclude that a local misappropriation is appropriate for resolution in state court. However, if the trade secret leaves the local jurisdiction, the trade secret owner may decide that a federal court provides a more effective chance to pursue relief. The owner may conclude that a remedy may be quicker in federal court particularly where many state courts are suffering from substantial civil case delays. The owner may conclude that litigation and other costs may be lower in federal court.

VI. Responding to Some Recent Questions About the Legislation

Some questions about the legislation have been raised. In reviewing the responses to these questions, in my view the benefits of the legislation are reinforced.

A. Promoting Litigation and Other Costs Savings

Some critics have suggested that a federal cause of action for trade secret misappropriation will adversely increase the length and cost of trade secret litigation. On the contrary, the legislation will result in significant cost reductions in a number of key respects and provide more options to reduce costs in trade secret cases. First, on those occasions in which the ex parte seizure order results in the recovery of stolen trade secrets, the cost savings will be tremendous. The timely recovery of the trade secrets will salvage the original investment in research and development of the trade secrets. It will also avoid the unauthorized copying and use of the trade secrets by others. This mechanism will minimize the costs and losses caused by

trade secret misappropriations and will address one of the paramount concerns of trade secret owners when their trade secrets are stolen.

Current law lacks this option. The inability to recover the stolen trade secrets in state court means the trade secrets may be used by others. Without the recovery of the stolen trade secrets, the thief reaps a windfall from the prior research and development invested in the trade secrets. The trade secret owner loses the competitive advantages from the confidentiality of the trade secret.

The legislation will also promote litigation costs savings. The costs of litigation will certainly turn on the facts and circumstances of the case and the jurisdiction in which the case is filed. In general, it takes longer, and there are more delays in state court. In many jurisdictions, it can take longer to obtain a trial in state court than federal court.¹⁰² Delay in obtaining a remedy is a significant cost by itself.

Once evidence crosses state lines, depositions or other discovery likely will fall outside of the court's jurisdiction and can only be reached with additional costs, expenses, and time. Under these circumstances, the state court process is usually cumbersome and more costly to obtain relief. The costs of litigation will be lower in federal court as a federal judge can order discovery and depositions, and enforce a judgment more efficiently and effectively than state courts.

Further cost savings will result from choices given to the trade secret owner by the legislation. The owner will be given a choice to pursue state or federal remedies depending on the circumstances. The owner may decide that a local misappropriation may be best for state court. To the extent cost may make a difference, the trade secret owner could pursue the least costly litigation option. So in a number of respects, the legislation will promote significant savings.

B. The Impact Of The New Seizure Order On Small Companies

Some have questioned the impact the court's seizure authority will have on small companies. First, the legislation will promote and protect trade secrets regardless of whether they are owned by small, medium and large companies as well as start-ups and individual. Small companies, like other entities will benefit from the ability to use the new seizure order provision. Many trade secrets are first developed in a small company or by individuals who have yet to form a company. In the event of trade secret theft, the small company can benefit by using the ex parte seizure provision to recover them through the federal court.

Second, the legislation contains several safeguards to prevent and address any abuse from the seizure provision. A court order will not issue unless the applicant makes the required showing to the satisfaction of the federal judge. The court, not a party to the action, takes custody of the trade secrets. The legislation includes restrictions about the publicity of the seizure which benefits those who might be unfairly targeted. Among other protections, the legislation establishes a private right of action for a person who suffers damage by a wrongful or excess seizure. The court can also award reasonable attorney's fees if it determines that a

misappropriation claim was made in bad faith. These protections will protect all companies or individuals.

C. “De-Harmonizing” State Trade Secret Law

Some have asked whether the federal legislation will “de-harmonize” state trade secret laws. The question misplaces the appropriate focus. The key issue is whether current law, which is based largely on a more-than-30-year-old statute, remains sufficient to address trade secret theft and misappropriation today. There is no reason trade secret law should be anchored to the past.

The federal legislation strengthens and modernizes trade secret law by addressing the technological realities and other challenges of today. The current federal criminal statute, the Economic Espionage Act of 1996, was originally based in large part on UTSA, which is the same model statute that 47 states have adopted in some form. UTSA was first promoted in 1979 and modified in 1985.

Many states have adopted variations to the UTSA model. For example, some states have criminal trade secret provisions and others do not. One challenge is that UTSA is now outdated in some key respects. A more-than-30-years-old statute model statute has not kept up with the technological advances and other challenges confronting trade secret law today particularly in our global and national economy. The legislation builds upon the UTSA framework to modernize and strengthen trade secret law. The failure to do so will allow the challenges in obtaining meaningful remedies under current law to persist, which is not acceptable.

Significantly, the legislation will not displace any state laws. There is no federal preemption. Instead, the legislation will provide another option to obtain remedies for trade secret misappropriation in federal court. In our global economy, the federal legislation is important given the role of trade secrets to commerce and because current state laws are often inadequate to address common challenges.

VII. Other Legislative Considerations

Two other issues deserve noting in considering the legislation.

A. Jurisdiction Also Based On Conduct

First, consideration should be given to including jurisdiction based on the interstate conduct related to the trade secret misappropriation.

The legislation provides federal jurisdiction based on “a trade secret that is related to a product or service used in, or intended for use in, interstate or foreign commerce.”¹⁰³ This language is based on the recent amendment to the EEA, under the Theft of Trade Secrets Clarification Act of 2012,¹⁰⁴ which was enacted to correct the limitations imposed under the *United States v. Aleynikov* Second Circuit case.¹⁰⁵

The current interstate standard can be augmented by a provision that clarifies that federal jurisdiction may be based on the transfer, in any manner, of a trade secret from one state to another state or outside the United States. Jurisdiction would then be based on either (a) the product or service intended for interstate or foreign commerce or (b) the interstate conduct in the case. The second option is similar to wire fraud,¹⁰⁶ which requires an interstate wire, and is based on the need for federal legislation to protect trade secrets removed from one state or the country. The current standard should cover most situations; language related to the transfer of the trade secret will remove any uncertainty and be consistent with the need for federal legislation.

B. Related Issue: Resolving The Circuit Split Under The Computer Fraud and Abuse Act

There is another issue that often arises in trade secret cases concerning the theft of confidential business information that is not a trade secret. In both criminal and civil cases, the defendant often misappropriates trade secrets along with other confidential business information. For example, the misappropriation may include financial, strategic and marketing information that may be useful to use and develop the stolen trade secrets. This information may not constitute trade secrets as defined under the EEA.

The Computer Fraud and Abuse Act (CFAA), first enacted in 1984,¹⁰⁷ is the primary federal computer statute that applies to the unauthorized obtaining or theft of information from a computer, along with related offenses. The CFAA provides for a civil private right of action for damages or equitable relief, along with potential criminal penalties.¹⁰⁸

The courts are presently divided on whether the CFAA applies when a trusted employee steals the company's confidential information using the company's computer.¹⁰⁹ The court split has persisted for more than six years.¹¹⁰ Consequently, the availability of a remedy depends on whether the jurisdiction applies a narrow or broad construction of the CFAA. Three circuits, including the First, Fifth and Eleventh Circuits, apply a broad construction which provides for a remedy for the theft of information by a computer.¹¹¹ However, two circuits, including the Fourth and Ninth Circuits, use a narrow interpretation and have held the CFAA does not cover this conduct.¹¹²

Because of the importance of confidential computer information, there should be a remedy when a trusted employee uses company computers to download, steal and transfer confidential business information either to start his own company or provide it to a competitor. The availability of a remedy for this theft should not turn on which jurisdiction the theft occurred.

In eventually addressing this problem, as part of a separate legislative reform apart from the current trade secret reform legislation, Congress has some options:

First, Congress can substitute a new standard which does not rely on "authorization" but instead focuses on the "use" or "purpose" to misuse the information. Several courts have considered this approach.

Second, Congress can use a misappropriation standard which would focus on whether the information was misappropriated or stolen. Initial authorized or unauthorized access to the information would not be dispositive. Instead, the facts concerning the intent and circumstances of the theft would determine whether the statute was violated.

Finally, if Congress is determined to retain the “authorization” standard, Congress should redefine the terms “without authorization” and “exceeds authorized access” to clarify that the statute applies when initial permitted access to information is later rescinded or abused. The current lack of clear guidance has resulted in disparate standards developed by the courts.

Insider theft of computer information should be covered under the CFAA. This type of conduct should not be subject to varying interpretations by the courts. Eventually this issue will need to be confronted. The problem arises in many trade secret cases but other cases too. I do not suggest that this issue be considered with the current legislation.

VIII. Reinforcing the Original Objectives of the EEA to Promote and Protect National and Economic Security

The EEA was enacted in 1996 to promote and protect national and economic security.¹¹³ As part of a bipartisan effort, the statute was enacted to fill in gaps under the law which previously allowed this conduct to go unpunished.¹¹⁴

In signing the EEA into law, President William J. Clinton noted:

Trade secrets are an integral part of virtually every sector of our economy and are essential to maintaining the health and competitiveness of critical industries operating in the United States. Economic espionage and trade secret theft threaten our Nation’s national security and economic well-being.¹¹⁵

The original objectives remain but in many respects, there are new risks and challenges to protect trade secrets. Since 1996, the role of trade secrets and information has expanded in ways that could not have been envisioned. In our global economy, trade secrets continue to play a vital role in the development of new products and services. However, without a meaningful ability for trade secret owners to recover their stolen trade secrets and obtain an adequate remedy, this key aspect of innovation is undermined.

The legislation will help modernize and strengthen trade secret law. It builds on the traditions of UTSA and addresses current issues and challenges. In my view, the legislation has strong bipartisan support and should be enacted.

Thank you for the opportunity to share my views on this important issue.

Endnotes:

¹ My statement is offered in my personal capacity based on my experience handling trade secret and foreign economic espionage cases and not on behalf of any organization or client. My views do not necessarily reflect the views of my firm, its clients, or my former employer, the U.S. Department of Justice.

² The National CHIP Program involves more than 250 federal prosecutors specially trained to prosecute cybercrime and intellectual property enforcement cases. For more on the history of the CHIP Program and DOJ cybercrime efforts, see Mark Krotoski, DOJ Cybercrime Efforts That Led To New Cybersecurity Unit, Law360 (Jan. 7, 2015), http://morganlewis.com/~media/law360_dojcybercrimeeffortsnewcybersecurityunit_07jan15.ashx.

³ Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488 (Oct. 11, 1996) (codified as amended in 18 U.S.C. §§ 1831–1839).

⁴ See U.S. Attorney's Manual § 9-59.100 ("The United States may not file a charge under 18 U.S.C. § 1831 of the Economic Espionage Act (hereinafter the 'EEA'), or use a violation under § 1831 of the EEA as a predicate offense under any other law, without the approval of the Assistant Attorney General for the National Security Division . . ."), <http://www.justice.gov/usam/usam-9-59000-economic-espionage>.

For a summary of the first eleven foreign economic espionage cases, see Appendix A; see also Mark L. Krotoski & Jenny Harrison, *Reviewing the First Foreign Economic Espionage Cases*, BNA'S PATENT, TRADEMARK & COPYRIGHT JOURNAL, 90 PTCJ 1951 (May 8, 2015) (summarizing the facts and proceedings for the first ten foreign economic espionage cases), http://www.morganlewis.com/~media/files/publication/outside%20publication/article/bbnainsight_foreigneconomic_espionage.ashx.

⁵ Redacted Plea Agreement at ¶ 2, *United States v. Meng*, No. 04-CR-20216 (N.D. Cal. Aug. 29, 2007, ECF Nos. 76, 77); Meng Government's Sentencing Memorandum at 5, 10–11 (June 11, 2008) (ECF No. 94).

⁶ Superseding Indictment at ¶¶ 28, 40, *United States v. Meng*, No. 04-CR-20216 (N.D. Cal. Dec. 17, 2004, ECF No. 57); Meng Redacted Plea Agreement at ¶ 2 (Aug. 29, 2007), ECF Nos. 76, 77); Meng Government's Sentencing Memorandum at 8 (June 11, 2008), ECF No. 94); Press Release, U.S. Dep't of Justice, Former Chinese National Charged with Stealing Military Application Trade Secrets from Silicon Valley Firm to Benefit Governments of Thailand, Malaysia, and China (Dec. 14, 2006), <http://www.justice.gov/archive/criminal/cybercrime/press-releases/2006/mengCharge.htm>.

⁷ Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR), 22 U.S.C. §§ 2778(b)(2), 2778(c), and 22 C.F.R. § 120.2.

⁸ Meng Redacted Plea Agreement at ¶ 2 (Aug. 29, 2007), ECF Nos. 76, 77; Meng Judgment (June 24, 2008), ECF No. 103; see generally Press Release, U.S. Dep't of Justice, Former Chinese National Convicted of Economic Espionage to Benefit China Navy Research Center (Aug. 2, 2007), http://www.justice.gov/archive/opa/pr/2007/August/07_nsd_572.html; Press Release, U.S. Dep't of Justice, Chinese National Sentenced For Committing Economic Espionage with the Intent to Benefit China Navy Research Center (June 18, 2008), <http://www.justice.gov/archive/criminal/cybercrime/press-releases/2008/mengSent.pdf>. According to court records, the sentence included a reduction based on substantial assistance provided under U.S.S.G. § 5K1.1. See Meng Sentencing Hearing Transcript at 10–11, 17–18 (June 18, 2008).

⁹ Huang Sentencing Hearing Transcript at 17, *United States v. Huang*, No. 10-CR-0102 (S.D. Ind. Dec. 22, 2011) (testimony of Dow AgroSciences managing counsel summarizing investigation); see also Press Release, U.S. Dep't of Justice, Chinese National Sentenced to 87 Months in Prison for Economic Espionage and Theft of Trade Secrets (Dec. 21, 2011), <http://www.justice.gov/opa/pr/chinese-national-sentenced-87-months-prison-economic-espionage-and-theft-trade-secrets>.

¹⁰ See Huang Plea Hearing Transcript at 41–43 (Oct. 18, 2011); Huang Sentencing Hearing Transcript at 18, 25 (Dec. 22, 2011); and Huang Plea Agreement ¶ 8(D).

¹¹ Defendant's Memorandum of Law in Support of Motion for Revocation of Detention at 6–7, *United States v. Kexue Huang*, No. 10-CR-0163 (S.D. Ind. Sept. 23, 2010), ECF No. 42; Huang Plea Agreement ¶ 8(A); Huang Government's Sentencing Memorandum at 10–11 (Dec. 12, 2011), ECF No. 91; Huang Sentencing Hearing Transcript at 23 (Dec. 22, 2011).

¹² Press Release, U.S. Dep't of Justice, Chinese National Charged with Economic Espionage Involving Theft of Trade Secrets from Leading Agricultural Company Based in Indianapolis (Aug. 31, 2010), <http://www.justice.gov/criminal/cybercrime/press-releases/2010/huangChar.pdf>.

¹³ Huang Plea Hearing Transcript (Oct. 18, 2011); Huang Plea Agreement; Order (March 8, 2011), ECF No. 72; *see also* Press Release, U.S. Dep’t of Justice, Chinese National Pleads Guilty to Economic Espionage and Theft of Trade Secrets (Oct. 18, 2011), <http://www.justice.gov/opa/pr/chinese-national-pleads-guilty-economic-espionage-and-theft-trade-secrets>.

¹⁴ *See* note 31, *infra*, for further information concerning *United States v. Philip Gabriel Pettersson aka “Stakkato”*, No. 09-CR-00471-RMW (N.D.Cal. May 5, 2009).

¹⁵ 14 U.L.A. 438 (1990). For the UTSA, *see* http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf. For UTSA jurisdictions, *see* [http://www.uniformlaws.org/LegislativeFactSheet.aspx?title=Trade Secrets Act](http://www.uniformlaws.org/LegislativeFactSheet.aspx?title=Trade%20Secrets%20Act).

¹⁶ 18 U.S.C. § 1839(3) (trade secret definition).

¹⁷ Center for Responsible Enterprise And Trade (CREAte.org) and PricewaterhouseCoopers LLP, Economic Impact of Trade Secret Theft: A Framework for Companies to Safeguard Trade Secrets and Mitigate Potential Threats, 3 (Feb. 2014), https://create.org/wp-content/uploads/2014/07/CREAte.org-PwC-Trade-Secret-Theft-FINAL-Feb-2014_01.pdf.

¹⁸ U.S. Bureau of Economic Analysis, National Income and Products Accounts, Gross Domestic Product: Third Quarter 2015 (Second Estimate), <http://www.bea.gov/newsreleases/national/gdp/gdpnewsrelease.htm>.

¹⁹ Under the Sentencing Guidelines, a variety of factors and measures may be considered such as the “reasonably foreseeable pecuniary harm”; the “fair market value of the property unlawfully taken, copied, or destroyed” or “the cost to the victim of replacing that property”; “the cost of developing that information or the reduction in value of that information that resulted from the offense.” U.S.S.G. § 2B1.1 cmt. n.3(A)(i), 3(C)(i), (ii).

²⁰ Restitution Order, *United States v. Kolon Industries, Inc.*, No. 12-CR-00137 (E.D. Va. April 30, 2015), ECF No. 194; Plea Agreement at ¶¶ 19–20 (E.D. Va. April 30, 2015) (restitution & fine), ECF No. 191; Judgment (E.D. Va. May 1, 2015), ECF No. 196; *see also* Press Release, U.S. Dep’t of Justice, Kolon Industries Inc. Pleads Guilty for Conspiring to Steal DuPont Trade Secrets Involving Kevlar Technology (Apr. 30, 2015), <http://www.justice.gov/opa/pr/kolon-industries-inc-pleads-guilty-conspiring-steal-dupont-trade-secrets-involving-kevlar>.

²¹ Government Sentencing Memorandum, at 22, 29–30, *United States v. Shanshan Du & Yu Qin*, No. 10-CR-20454 (E.D. Mich. April 25, 2013) (ECF No. 185). Government Sentencing Memorandum at 22, 29–30, *United States v. Shanshan Du & Yu Qin*, No. 10-CR-20454 (E.D. Mich. April 25, 2013), ECF No. 185.

²² Entry of Judgment, *UniRAM Technology, Inc. v. Taiwan Semiconductor Manufacturing Co.* at *2–3, No. 04-CV-01268 (N.D. Cal. April 17, 2008), ECF No. 628 (Plaintiff’s damages expert estimated Defendant generated over \$185 million in profits off the accused products, while Defendant’s expert used a different accounting method for calculating revenues and costs, arriving at a profit figure of \$78.6 million, of which only a portion was attributable to the misappropriated memory macros.).

²³ Government’s Sentencing Memorandum at 4, *United States v. Chung*, No. 08-CR-00024 (C.D. Cal. Feb. 11, 2010), ECF No. 156 (estimating the loss to be around \$35 million based on Boeing’s research and development expenditure of over \$35 million to develop the trade secret and noting the Probation estimate of over \$20 million); *see also* Memorandum of Decision, *United States v. Chung*, 633 F. Supp. 2d 1134 (C.D. Cal. 2009), *aff’d*, 659 F.3d 815 (9th Cir. 2011) (affirming conviction and sentence).

²⁴ *See* Defendant’s Sentencing Memorandum at 3, *United States v. Agodoa*, No. 13-CR-20525 (E.D. Mich. Jan. 14, 2014), ECF No. 27 (agreeing with loss estimate obtained from Wacker Chemical Corporation grand jury probation for the recommended sentence).

²⁵ Plea Hearing at *33, *United States v. Huang*, No. 10-CR-0102 (S.D. Ind. Oct. 18, 2011), 11-CR-00163 (D. Minn. Dec. 21, 2011); Sentencing Hearing at *7, 32, *United States v. Huang*, No. 10-CR-0102 (S.D. Ind. Dec. 21, 2011), 11-CR-00163 (D. Minn. Dec. 21, 2011).

²⁶ *United States v. Williams*, No. 06-CR-313 (N.D. Ga. May 23, 2007) (intended loss of \$1.5 million was determined to “under represent the seriousness of the offense”), *aff’d*; 526 F.3d 1312, 1321 n.2 (11th Cir. 2008) (affirming conviction and sentence; concluding “the district court did not err by considering” Coca-Cola’s annual revenues “in deciding whether the \$1.5 million intended loss calculated under the guidelines underrepresented the seriousness of the offense”).

²⁷ Exec. Order, “Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities” (Apr. 1, 2015), <https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m>.

- ²⁸ Press Release, Federal Bureau of Investigation, Update on Sony Investigation (December 19, 2014), <http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation>.
- ²⁹ Press Release, U.S. Dep’t of Justice, Four Members of International Computer Hacking Ring Indicted for Stealing Gaming Technology, Apache Helicopter Training Software (Sept. 30, 2014), <http://www.justice.gov/opa/pr/four-members-international-computer-hacking-ring-indicted-stealing-gaming-technology-apache>.
- ³⁰ Indictment, *United States v. Wang Dong et al.* No. 14-CR-118 (W.D. Pa. May 2014), <http://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf>; see also Press Release, U.S. Dep’t of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), <http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor>.
- ³¹ Indictment, *United States v. Philip Gabriel Pettersson aka “Stakkato”* No. 09-CR-00471-RMW (N.D. Cal. May 5, 2009), http://www.wired.com/images_blogs/threatlevel/2009/05/petterssonindictment.pdf; see also Dan Goodin, Sweden to Prosecute Alleged Cisco, NASA Hacker, THE REGISTER (Feb. 8, 2010), http://www.theregister.co.uk/2010/02/08/swedish_hacker_prosecution.
- ³² See, e.g., Mandiant: *APT1 Exposing One of China’s Cyber Espionage Units* (2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf; FireEye, *APT28: A Window Into Russia’s Cyber Espionage Operations?* at 3 (2015), <https://www2.fireeye.com/apt28.html>; Office of the National Counterintelligence Executive: Foreign Spies Stealing U.S. Economic Secrets in Cyberspace (Oct. 2011), http://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.
- ³³ On the civil remedies factor, U.S. Department of Justice policy clarifies that: “The availability of a civil remedy should not be the only factor considered in evaluating the merits of a referral because the victim of a trade secret theft almost always has recourse to a civil action. The universal application of this factor would thus defeat the Congressional intent in passing the EEA.” U.S. Attorney’s Manual § 9-59.100, <http://www.justice.gov/usam/usam-9-59000-economic-espionage>.
- ³⁴ U.S. Attorney’s Manual § 9-59.100 (listing factors), <http://www.justice.gov/usam/usam-9-59000-economic-espionage>. See also Tom Reilly, Economic Espionage Charges Under Title 18 U.S.C. § 1831: Getting Charges Approved and the “Foreign Instrumentality” Element, 57 UNITED STATES ATTORNEYS’ BULLETIN 2, 12–13 (Nov. 2009) (describing review process), <http://www.justice.gov/sites/default/files/usao/legacy/2009/12/10/usab5705.pdf>.
- ³⁵ See, e.g., Cal. Penal Code § 499c (trade secret theft may result in a criminal fine up to \$5,000 and up to one year in jail); Nev. Rev. Stat. § 600A.035 (trade secret theft is punishable by “a minimum term of not less than 1 year and a maximum term of not more than 10 years” in prison and “a fine of not more than \$10,000”); RCW § 9A.56.010(6) (defining “deprive,” under the theft and robbery statute, to include the “unauthorized use or an unauthorized copy of records, information, data, trade secrets, or computer programs”); Tex. Penal Code § 31.05 (at least two years imprisonment and up to a maximum of 10 years and a fine of up to \$10,000).
- ³⁶ States have recognized this problem. Several states have adopted the Uniform Interstate Depositions and Discovery Act. However, many states have not, including Texas and Florida. See Legislative Fact Sheet - Interstate Depositions and Discovery Act (listing states), <http://www.uniformlaws.org/Act.aspx?title=Interstate%20Depositions%20and%20Discovery%20Act>.
- ³⁷ Fed. R. Civ. P. 45(b)(2) (“A subpoena may be served at any place within the United States”).
- ³⁸ See 28 U.S.C. §§ 1331 (federal question), 1332 (diversity of citizenship).
- ³⁹ See also U.S. CONST. art. III, § 2 (“The judicial power shall extend to all Cases, in Law and Equity . . . between Citizens of different States.”).
- ⁴⁰ 28 U.S.C. §§ 1331 (federal question); see also U.S. CONST. ART. III, § 2 (federal courts can hear “all cases, in law and equity, arising under this Constitution, [and] the laws of the United States”).
- ⁴¹ 18 U.S.C. § 1030(g) (limited civil cause of action).
- ⁴² Mark Krotoski, *Viewpoint: Time to Reform the Computer Fraud and Abuse Act*, THE RECORDER (Nov. 18, 2015) (noting circuit split and need for reform), <http://www.therecorder.com/home/id=1202742832060/Viewpoint-Time-to-Reform-the-Computer-Fraud-and-Abuse-Act?slreturn=20151021171349>; Mark Krotoski & Brock Dahl: *Stealing Trade Secrets and Confidential Information With Computers*, BNA’S PATENT, TRADEMARK & COPYRIGHT JOURNAL, 89 PTCJ 1142 (Feb. 27, 2015) (same).
- ⁴³ 28 U.S.C. § 1367 (supplemental jurisdiction).
- ⁴⁴ Mark Krotoski, *Common Issues and Challenges in Prosecuting Trade Secret and Economic Espionage Act Cases*, 57 UNITED STATES ATTORNEYS’ BULLETIN 2, 12–13 (Nov. 2009) (describing reactive nature of trade secret investigations), <http://www.justice.gov/sites/default/files/usao/legacy/2009/12/10/usab5705.pdf>.

⁴⁵ See generally Mark Krotoski, Identifying And Using Electronic Evidence Early To Investigate And Prosecute Trade Secret And Economic Espionage Act Cases, 57 UNITED STATES ATTORNEYS' BULLETIN 42-51 (Nov. 2009) (noting cases involving the use of computers and emails to obtain and transfer trade secrets), http://www.justice.gov/criminal/cybercrime/docs/prosecuting_ip_crimes_manual_2013.pdf.

⁴⁶ Press Release, U.S. Dep't of Justice, Former DuPont Chemist Sentenced to 14 Months in Prison for Stealing DuPont Trade Secrets (Oct. 21, 2010), <https://www.fbi.gov/baltimore/press-releases/2010/ba102110a.htm>.

⁴⁷ Press Release, U.S. Dep't of Justice, Two Engineers Found Guilty of Stealing Goodyear Trade Secrets (Dec. 9, 2010) (noting that "the defendants used a cell phone camera to surreptitiously take seven unauthorized photographs of a Goodyear swab down device" and "then emailed the unauthorized photographs to employees at a Wyko subsidiary located in Dudley, England"), <http://www.justice.gov/opa/pr/two-engineers-found-guilty-stealing-goodyear-trade-secrets>.

⁴⁸ Press Release, U.S. Dep't of Justice, Former Connecticut Resident Pleads Guilty to Attempting to Send Sensitive Military Documents to Iran (Feb. 25, 2015) (noting the defendant "corresponded by email with an individual in Iran to whom he attempted to send, and in some cases did send, documents containing trade secret, proprietary and export controlled material relating to the Joint Strike Fighter Program"), <http://www.justice.gov/opa/pr/former-connecticut-resident-pleads-guilty-attempting-send-sensitive-military-documents-iran>; Government's Sentencing Memorandum at 5-6, *United States v. David Kent Lewis*, No. 14-CR-00014 (E.D. Ky. Oct. 8, 2014), ECF No. 19; Judgment (E.D. Ky. Oct. 8, 2014), ECF No. 21; see also Press Release, U.S. Dep't of Justice, Former Winchester Brake Pad Engineer Pleads Guilty to Theft of Trade Secrets Charge (March 5, 2014) (noting the defendant "emailed trade secrets concerning the specifications of brake pads" and "was paid thousands of dollars by a Canadian company for this information"), <http://www.justice.gov/usao-edky/pr/former-winchester-brake-pad-engineer-pleads-guilty-theft-trade-secrets-charge>.

⁴⁹ 1996 House Report, at 4 (noting "threats to the nation's economic interest are threats to the nation's vital security interests").

⁵⁰ See 17 U.S.C. §§ 501 *et seq.*

⁵¹ See Lanham Act, 15 U.S.C. §§ 1051-1127.

⁵² See U.S. Patent Act, 35 U.S.C. §§ 1 *et seq.*

⁵³ Federal criminal statutes already apply to copyright and trademark infringement and trade secret misappropriation. Criminal copyright cases are authorized under 17 U.S.C. § 506(a) and 18 U.S.C. § 2319; criminal trademark cases are provided for under 18 U.S.C. § 2320. Trade secret misappropriation is subject to criminal penalties under the Economic Espionage Act, 18 U.S.C. §§ 1831-1839.

⁵⁴ See 17 U.S.C. § 102(a) (subject matter of copyright).

⁵⁵ See 15 U.S.C. § 1127 (defining "trademark").

⁵⁶ 35 U.S.C. § 154(a) (contents and term of patent).

⁵⁷ *Coca-Cola Bottling Co. of Shreveport, Inc. v. Coca-Cola Co.*, 107 F.R.D. 288, 289 (1985) ("The formula for Merchandise 7X has been tightly guarded since Coca-Cola was first invented and is known by only two persons within The Coca-Cola Company.... The only written record of the secret formula is kept in a security vault at the Trust Company Bank in Atlanta, Georgia, which can only be opened upon a resolution from the Company's Board of Directors.").

⁵⁸ *Coca-Cola Co. v. Koke Co. of America*, 254 U.S. 143, 145 (1920) (in trademark infringement action, summarizing prior trademarks); *United States v. Coca Cola Co. of Atlanta*, 241 U.S. 265, 272 (1916) (describing the registered trademark of "Coca Cola" in the 1890s); *Coca-Cola Company v. Gemini Rising, Inc.*, 346 F. Supp. 1183, 1186 (E.D.N.Y. 1972) (in injunction for "Coca-Cola" trademark, noting trademarks filed in 1893, 1905, and 1928).

⁵⁹ The Coca-Cola logo story, <http://www.coca-cola.co.uk/stories/history/advertising/the-logo-story>.

⁶⁰ U.S. Registration Number: 696147 (1960) (bottle),

http://tsdr.uspto.gov/#caseNumber=72069873&caseType=SERIAL_NO&searchType=statusSearch; see also *Qualitex Co. v. Jacobson Products Co.*, 514 U.S. 159, 162 (1995) (noting that the "courts and the Patent and Trademark Office have authorized for use as a mark a particular shape (of a Coca-Cola bottle),"); see generally Coke Lore: Trademark Chronology, <http://www.coca-colacompany.com/stories/coke-lore-trademark-chronology>.

⁶¹ See U.S. Design Patent No. 48160 (1915), <http://www.google.com/patents/USD48160>; see also The Story of the Coca-Cola Bottle (Feb. 26, 2015), <http://www.coca-colacompany.com/stories/the-story-of-the-coca-cola-bottle>.

⁶² S. 1890 § 2 (proposed § 1836(b)(2)(A)(i)).

⁶³ *Id.* § 1836(b)(2)(A).

⁶⁴ *Id.* § 1836(b)(2)(B).

⁶⁵ *Id.* § 1836(b)(2)(E).

⁶⁶ *Id.* § 1836(b)(2)(D).

⁶⁷ *Id.* § 1836(b)(2)(D).

⁶⁸ *Id.* §§ 1836(b)(2)(B)(iv), (F)(i).

⁶⁹ *Id.* § 1836(b)(2)(F)(ii).

⁷⁰ *Id.* § 1836(b)(2)(F)(iii).

⁷¹ *Id.* § 1836(b)(2)(G).

⁷² *See, e.g., Homecare CRM, LLC v. Adam Group, Inc.*, 952 F. Supp. 2d 1373, 1380 (N.D. Ga. 2013) (Rule 11 sanctions ordered when “the factual allegations in support of Homecare’s trade-secrets claim do not, and did not at the time this action was filed, have evidentiary support...”); *see also Qad., inc. v. ALN Assoc., Inc.*, 18 U.S.P.Q. 2d 1122 (N.D. Ill. 1990) (dismissing Qad’s trade secret count and awarding Rule 11 sanctions to defendant based on Qad’s persistent failure to identify a claim); *Robertshaw Controls Co. v. Weerstra*, 1990 U.S. Dist. LEXIS 17380 at *16 (W.D. Mich. 1990) (ordering Rule 11 sanctions when “[a]lthough the Court has concluded that it was at least reasonable to file the complaint, further investigation of the facts would have revealed that defendant never stole any confidential information or trade secrets”).

⁷³ S. 1890 § 2 (proposed § 1836(b)(3)(D)).

⁷⁴ *Id.* § 1836(b)(2)(D).

⁷⁵ *Id.*

⁷⁶ *Id.* § 1836(b)(2)(H).

⁷⁷ *See, e.g., Cal. Penal Code § 499c* (trade secret theft may result in a criminal fine up to \$5,000 and up to one year in jail); *Nev. Rev. Stat. § 600A.035* (trade secret theft is punishable by “a minimum term of not less than 1 year and a maximum term of not more than 10 years” in prison and “not more than \$10,000”); *RCW § 9A.56.010(6)* (defining “deprive,” under the theft and robbery statute, to include the “unauthorized use or an unauthorized copy of records, information, data, trade secrets, or computer programs”); *Tex. Penal Code § 31.05* (at least two years imprisonment and up to a maximum of 10 years and a fine of up to \$10,000).

⁷⁸ 1996 House Report, at 7.

⁷⁹ 142 CONG. REC. H10462 (Sept. 17, 1996).

⁸⁰ *Id.* S12212 (daily ed. Oct. 2, 1996).

⁸¹ *Id.* S12213 (daily ed. Oct. 2, 1996) (Manager’s Statement).

⁸² *Id.*

⁸³ UTSA, Section 5 provides that “a court shall preserve the secrecy of an alleged trade secret by reasonable means, which may include granting protective orders in connection with discovery proceedings, holding in-camera hearings, sealing the records of the action, and ordering any person involved in the litigation not to disclose an alleged trade secret without prior court approval.”

⁸⁴ 18 U.S.C. § 1835 provides: “In any prosecution or other proceeding under this chapter, the court shall enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws. An interlocutory appeal by the United States shall lie from a decision or order of a district court authorizing or directing the disclosure of any trade secret.”

⁸⁵ *See generally Mohawk Industries, Inc. v. Carpenter*, 558 U.S. 100 (2009) (holding interlocutory appellate review of an adverse attorney-client privilege ruling was not available and reinforcing the role of one appeal following a final judgment in the case).

⁸⁶ *See United States v. Hsu*, 155 F.3d 189, 203-04 (3d Cir. 1998) (reversing disclosure order as the attempt and conspiracy offenses did not require actual proof of the trade secret); *see also United States v. Fei Ye*, 436 F.3d 1117, 1121 (9th Cir. 2006) (although the circuit lacked jurisdiction over the interlocutory appeal since “the district court’s order does not direct or authorize the ‘disclosure’ of trade secrets as required by the plain language of § 1835,” issuing a writ of mandamus to rescind the district court ruling mandating pretrial depositions concerning the trade secrets).

⁸⁷ 18 U.S.C. § 1839(3).

⁸⁸ 1996 House Report, at 12; *see also United States v. Chung*, 659 F.3d 815 (9th Cir. 2011) (noting that the EEA trade secret definition “is derived from the definition that appears in the Uniform Trade Secrets Act” and “we consider instructive interpretations of state laws that adopted the UTSA definition without substantial modification”) (footnote omitted); *Hsu*, 155 F.3d at 196 (“The EEA’s definition of a ‘trade secret’ is similar to that found in a number of state civil statutes and the Uniform Trade Secrets Act (‘UTSA’), a model ordinance which permits civil actions for the misappropriation of trade secrets. There are, though, several critical differences which serve to broaden the EEA’s scope.”) (footnote omitted).

⁸⁹ See generally *Ratzlaf v. United States*, 510 U.S. 135, 147-48 (1994) (“we do not resort to legislative history to cloud a statutory text that is clear”).

⁹⁰ UTSA, § 1(4).

⁹¹ 18 U.S.C. § 1839(3).

⁹² 1996 House Report, at 12 (“These general categories of information are included in the definition of trade secret for illustrative purposes and should not be read to limit the definition of trade secret. It is the Committee’s intent that this definition be read broadly.”).

⁹³ 1996 House Report, at 11; see also *id.* at 4 (“In the last few decades, intangible assets have become more and more important to the prosperity of companies.... As the nation moves into the high-technology, information age, the value of these intangible assets will only continue to grow.”).

⁹⁴ 18 U.S.C. § 1837 (applicability to conduct outside the United States); see also 1996 House Report, at 14 (“To rebut the general presumption against the extraterritoriality of U.S. criminal laws, this subsection makes it clear that the Act is meant to apply to the specified conduct occurring beyond U.S. borders.”).

⁹⁵ See generally *Kiobel v. Royal Dutch Petroleum Co.*, 133 S.Ct. 1659, 1664-65 (2013) (applying presumption to the Alien Tort Statute); *Morrison v. National Australia Bank Ltd.*, 130 S.Ct. 2869, 2878 (2010) (noting “[w]hen a statute gives no clear indication of an extraterritorial application, it has none”).

⁹⁶ See UTSA, § 6.

⁹⁷ 18 U.S.C. § 1838.

⁹⁸ Why States Should Adopt USA, Uniform Law Commission, National Conference of Commissioners on Uniform State Laws (last visited Dec. 1, 2015), <http://www.uniformlawcommission.com/Narrative.aspx?title=Why%20States%20Should%20Adopt%20USA>.

⁹⁹ Age Discrimination in Employment Act (ADEA), 29 U.S.C. §§ 621-634.

¹⁰⁰ See State Computer Crime Statutes, National Conference of State Legislatures (last updated June 12, 2015) (listing state statutes), <http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx>.

¹⁰¹ 18 U.S.C. § 1030 *et seq.*

¹⁰² For example, fewer than 66% of California civil unlimited cases were disposed of in less than 12 months and 16% remained pending after 24 months for the financial year 2014. 2015 Court Statistics Report, Statewide Caseload Trends 2004-2005 Through 2013-2014, Judicial Council of California, page 71 (available at <http://www.courts.ca.gov/documents/2015-Court-Statistics-Report.pdf>). On the other hand, the average time from filing to disposition for civil cases in federal court for the year ending on June 30, 2015 was 8.8 months and only 8.9% of civil cases were over three years old. U.S. District Courts – Combined Civil and Criminal Federal Court Management Statistics, United States Courts (Dec. 31 2014) (available at <http://www.uscourts.gov/statistics/table/na/federal-court-management-statistics/2015/06/30-3>).

¹⁰³ S. 1890 § 2 (proposed § 1836(b)(1)).

¹⁰⁴ Theft of Trade Secrets Clarification Act, Pub. L. No. 112-236, § 2, 126 Stat. 1627 (2012), <https://www.congress.gov/112/plaws/publ236/PLAW-112publ236.pdf>.

¹⁰⁵ *United Staes. v. Aleynikov*, 676 F.3d. 71 (2d Cir. 2012).

¹⁰⁶ 18 U.S.C. § 1343 (wire fraud).

¹⁰⁷ 18 U.S.C. § 1030. Section 1030 was originally enacted in 1984. See Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, § 2102(a), 98 Stat. 2190, 2190–92 (codified at 18 U.S.C. § 1030 *et seq.*).

¹⁰⁸ 18 U.S.C. § 1030(g) (civil private right of action). Congress added the private right of action in 1994. See Pub. L. 103–322, title XXIX, § 290001(b)–(f), Sept. 13, 1994, 108 Stat. 2097–2099.

¹⁰⁹ See, e.g., M. Krotoski & B. Dahl, Stealing Trade Secrets and Confidential Information With Computers: Time to Resolve the Lingering Circuit Split, BNA’s Patent, Trademark & Copyright Journal, 89 PTCJ 1142 (Feb. 27, 2015) (89 PTCJ 1142, 2/27/15) (reviewing circuit split).

¹¹⁰ See, e.g., *LVRC Holdings LLC, v. Brekka*, 581 F.3d 1127, 1134-35 (9th Cir. 2009) (noting disagreement with Seventh Circuit construction); see also *United States v. John*, 597 F.3d 263, 269 (5th Cir. 2010) (noting disagreement with Ninth Circuit construction of the CFAA); *Orbit One Communications, Inc. v. Numerex Corp.*, 692 F. Supp. 2d 373, 385 & nn. 65-66 (S.D.N.Y. 2010) (noting the division among federal circuit and district court cases construing the CFAA).

¹¹¹ See *United States v. Rodriguez*, 628 F.3d 1258, 1260 (11th Cir. 2010); *United States v. John*, 597 F.3d 263, 269 (5th Cir. 2010); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st 2001).

¹¹² *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 202 (4th Cir. 2012), *cert. dismissed*, 133 S.Ct. 831 (2013) (No. 12-518); *United States v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012) (en banc).

¹¹³ Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488 (Oct. 11, 1996) (codified as amended in 18 U.S.C. §§ 1831–1839).

¹¹⁴ 1996 House Report, at 4 (noting “the nation’s economic interests are part of its national security interests” and “threats to the nation’s economic interest are threats to the nation’s vital security interests”); *id.* at 6-7 (noting gaps under federal law); *see also* *United States v. Hsu*, 155 F.3d 189, 194 (3d Cir. 1998) (noting prior to the EEA “the absence of any comprehensive federal remedy targeting the theft of trade secrets, compelling prosecutors to shoehorn economic espionage crimes into statutes directed at other offenses”).

¹¹⁵ President William J. Clinton, Presidential Statement on the Signing of the Economic Espionage Act of 1996 (Oct. 11, 1996), available at 1996 Pub. Papers 1814 (Oct. 11, 1996), <http://www.gpo.gov/fdsys/pkg/WCPD-1996-10-14/pdf/WCPD-1996-10-14-Pg2040-2.pdf>.

Appendix A

Summary of the First Eleven Foreign Economic Espionage Cases

Under 18 U.S.C. § 1831

(1996 – 2015)

Appendix A
Summary of the First Eleven Foreign Economic Espionage Cases Under 18 U.S.C. § 1831 (1996 – 2015)

Case	Case	Court; Case No.	Defendant: Disposition	Date of Misappro.	Date of Indictment	Date of Disposition	Trade Secret	Theft of Secret	Foreign Government Connection	Sentence
1	Okamoto	NDOH; No. 01-CR-00210	Okamoto: fugitive Serizawa: plea conviction: §1001 (1 count)	1999	May-01	NA	Trade secrets regarding DNA & cell line reagents	Employee stole trade secrets from his employer, sent them to Serizawa for holding, then took a new position at a state-funded research institute in Japan.	Japanese state-funded research institute	Okamoto: A fugitive Serizawa: 3 yrs probation, 150 hrs community service; \$500 fine
2	Fei Ye	NDCA; No. 02-CR-20145	Fei Ye: plea conviction: §1831 (2 counts); acquittals: §1832 (3 counts); §371 (1 count); §2314 (2 counts) Zhong: plea conviction: §1831 (2 counts); acquittals: §1832 (4 counts); §371 (1 count); §2314 (2 counts)	2001	Dec-02	Dec-06	Trade secrets regarding the design and manufacture of computer microprocessors	Employees stole employer's trade secrets and planned to use them at their PRC-funded company, but were stopped at the airport with the secrets.	PRC state-funded private company	Both: 366 days in prison, 3 yr supervised release
3	Meng	NDCA; No. 04-CR-20216	Meng: plea convictions: §1831 (1 count); 22 USC § 2778 (1 count); acquittals: §2314 (14 count); §371 (3 counts); §1831 (2 counts); §2778 (1 count); §1832 (12 counts); §1001 (3 counts)	2003	Dec-04	Aug-07	Trade secrets regarding visual simulation software program	Employee took employer's trade secrets to new job in the PRC. He was stopped at the airport with the secrets when traveling to the US on a business trip.	PRC Navy Research Center	24 months + 1 day in prison, 3 yr supervised release; \$10,200 fine
4	Lee	NDCA; No. 06-CR-00424	Lee: jury trial acquittal: §1831 (3 counts); §1832 (4 counts) Ge: jury trial acquittal: §1831 (3 counts); §1832 (4 counts)	2003	Sep-07	Dec-09	Trade secrets regarding computer chip designs and manufacturing information	Employees allegedly stole trade secrets from two former employers to use at their own company.	Private company seeking PRC state-funding	NA
5	Chung	CDCA; No. 08-CR-00024	Chung: bench trial conviction: §1831 (6 counts), §951 (1 count), §371 (1 count); §1001 (1 count); acquittals: §1831 (2 counts); §1512 (1 count); §1001 (2 counts)	2003-2006	Feb-08	Jul-09	Trade secrets regarding space shuttle and Delta IV rocket	Employee stole two former employers' trade secrets	PRC military	188 months in prison
6	Jin	NDIL; No. 08-CR-00192	Jin: bench trial conviction: §1832 (3 counts); acquittal: §1831 (3 counts)	2007	Apr-08	Nov-11	Trade secrets regarding iDEN mobile communications technology	Employee stole employer's trade secrets and planned to take them to the PRC to work for a company connected to the PRC military, but was stopped at the airport with the documents.	PRC military	4 years in prison; \$20,000 fine
7	Huang	SDIN; No. 10-CR-0102	Huang: plea conviction: §1831 (1 count); acquittal: §1831 (11 counts); §2314 (5 counts)	2007-2010	Jun-10	Oct-11	Trade secrets regarding insecticides	Employee stole employer's trade secrets, transferred them to the PRC and Germany, and worked at a PRC university to further develop them.	PRC state-funded research institute	87 months in prison
8	Doxer	D.Mass; No. 11-CR-10268	Doxer: plea conviction: §1831 (1 count)	2006	Jul-11	Aug-11	Confidential company information (contractual papers, customer lists, and employee lists)	Employee stole documents he had access too. Only sting-operation case.	Israel	6 months prison; 6 months home confinement; \$25,000 fine
9	Liew	NDCA; No. 11-CR-00573	Maegerle: jury trial conviction: §1832 (3 counts), §1512 (1 count) Chao: plea conviction: §1831 (1 count) C. Liew: pending trial	1998-2008	Feb-12	2014	Trade secrets regarding pigment manufacturing processes	Employees stole employer's trade secrets and used them to obtain contracts with PRC companies.	PRC state-funded company	Liew: 180 mths in prison; Maegerle: 18 mths; Both: forfeit \$27.8M

Appendix A
Summary of the First Eleven Foreign Economic Espionage Cases Under 18 U.S.C. § 1831 (1996 – 2015)

Case	Case	Court; Case No.	Defendant: Disposition	Date of Misappro.	Date of Indictment	Date of Disposition	Trade Secret	Theft of Secret	Foreign Government Connection	Sentence
10	Dong	WDPA; No. 14-CR- 118	All 5 defendants (Dong, Kailiang, Xinyu, Zhenyu, Chunhui) are fugitives and the 31-count indictment is pending	2006-2014	May-14	NA	information including emails regarding business strategies, financial positions, and production capabilities	Cyber-espionage: alleged hacking of company computer systems through spear-phishing emails	PRC military	NA
11	Pang	NDCA; No. 15-CR- 106	Hao Zhang: arrested on 5/16/2015 Remaining 5 defendants (Pang, Huisui Zhang, Chen, Gang, Zhou) are fugitives and the 32-count indictment is pending	2006-2015	Apr-15	NA	Confidential thin-film bulk acoustic resonator ("FBAR") technology	Employees allegedly stole employers' trade secrets and used them to obtain business with a PRC-sponsored university to further develop the technology.	PRC state-funded research institute	NA

Appendix B

Trade Secret Examples Based on Recent

Criminal and Civil Cases

Appendix B
Trade Secret Examples
Based on Recent Criminal and Civil Cases

No.	Trade Secret	Trade Secret Owner	Industry	Conduct and Case Disposition
1	“Inbred” or “parent” line of corn seed information	U.S. seed companies DuPont Pioneer, Monsanto, and LG Seeds, located in Iowa, Missouri, and Indiana respectively and utilizing facilities in Iowa, Illinois, and Indiana ¹	Agriculture	• <i>Criminal case</i> • <i>Alleged Conduct:</i> Third Superseding Indictment alleges the defendants conspired to steal trade secrets of seed manufacturing companies, and transport them to China to use in their China-based seed company • <i>Disposition:</i> Case remains pending²
2	Proprietary organic insecticides	Dow AgroSciences, headquartered in Indiana ³	Agriculture	• <i>Criminal case</i> • <i>Conviction:</i> Defendant who served as a research scientist and leader for strain development pled guilty to stealing his employer’s trade secrets and further developing them as his position as visiting professor at Hunan Normal University in the PRC • <i>Disposition:</i> Sentenced to serve 87 months in prison⁴
3	Computer-assisted drawing software for airplane parts, including aircraft brake assembly and specifications	Replacement Aircraft Parts Co. (RAPCO) located in Wisconsin	Airplane parts	• <i>Criminal case</i> • <i>Bench Trial Conviction:</i> Defendant convicted under 18 U.S.C. § 1832 for stealing his employer’s data and attempting to sell it to a competitor • <i>Disposition:</i> Sentenced to 30 months in prison and \$2,500 fine; conviction affirmed on appeal⁵
4	Hybrid motor technology	General Motors located in Michigan ⁶	Automobile	• <i>Criminal case</i> • <i>Jury Trial Conviction:</i> A former General Motors engineer (Yu Qin) and her husband (Shanshan Du) were convicted at a jury trial for copying 16,000 GM computer files which included trade secrets, with the intent to use them in a joint venture with an automotive competitor in China under 18 U.S.C. § 1832(a)(3), (a)(5) and other counts • <i>Disposition:</i> Qin was sentenced to three years in prison and a \$25,000 fine and Du was sentenced to a year and a day in prison and a \$12,500 fine⁷; the trial convictions and sentences were affirmed on appeal⁸

No.	Trade Secret	Trade Secret Owner	Industry	Conduct and Case Disposition
5	Brake pad specifications	Brake Parts International, Inc., headquartered in Illinois, with production in Kentucky ⁹	Automobile	• <i>Criminal case</i> • <i>Conviction:</i> Defendant pled guilty to one count of conspiring to commit theft of trade secrets under 18 U.S.C. § 1832(a)(5) for emailing brake pad formulations and providing trade secret information to a competitor • <i>Disposition:</i> Sentenced to three years probation, nine months home incarceration, and \$32,000 in restitution¹⁰
6	Coca Cola® marketing information, product sample	Coca Cola, headquartered in Georgia	Beverage	• <i>Criminal case</i> • <i>Jury Trial Conviction:</i> Lead defendant employee convicted in a jury trial for misappropriating Coca Cola's trade secrets and attempting to sell them for profit to a competitor • <i>Disposition:</i> Sentenced to 96 months in prison and ordered to pay restitution of \$40,000¹¹ • <i>Other Convictions:</i> Co-defendants: <i>United States v. Dimson</i> (sentenced June 5, 2007, to 60 months and \$40,000 restitution following plea to conspiracy)¹²; <i>United States v. Duhaney</i> (sentenced June 5, 2007, to 24 months and \$40,000 restitution following plea to conspiracy and included a downward departure for substantial assistance under U.S.S.G. § 5K1.1)¹³

No.	Trade Secret	Trade Secret Owner	Industry	Conduct and Case Disposition
7	Kevlar® technology used for body armor, fiberoptic cables, automotive and industrial products	E.I. DuPont de Nemours & Co., headquartered in Delaware, and manufactured in Virginia, Ireland, and Japan	Chemical	• <i>Criminal case</i> • <i>Conviction:</i> South Korean company pled guilty to conspiring with former DuPont employees to steal trade secrets with the intent to improve the company's own para-aramid fiber product under 18 U.S.C. § 1832(a)(5) • <i>Disposition:</i> Sentenced to pay an \$85 million fine, \$275 million in restitution and to serve a five year term of corporate probation¹⁴ • <i>Civil Case</i> • Complaint alleges a South Korean company attempted to obtain and use DuPont's confidential and proprietary manufacturing process for Kevlar® technology for its own products and processes • <i>Disposition:</i> The parties agreed to settle, and the case was dismissed. Kolon agreed to make up-front and ongoing payments to DuPont. Additional details of the settlement agreement are confidential.¹⁵
8	Chemical formulas used in the manufacture of silicone-based and rubber products	Wacker Chemical Corporation, located in Michigan	Chemical	• <i>Criminal case</i> • <i>Conviction:</i> Defendant pled guilty to one count of theft of trade secrets under 18 U.S.C. § 1832(a)(3) for transmitting and disclosing more than 100 confidential chemical formulas to a South Korean-based chemical company • <i>Disposition:</i> Sentenced to 24 months in prison and a \$7,500 fine¹⁶
9	Technical drawings, software, and tools for post-tensioning materials for buildings and foundations	Suncoast Post-Tension, Ltd.	Construction	• <i>Civil case</i> • Texas federal jury awarded \$24.5 million to Suncoast. • \$13.5 million in punitive damages, \$8 million in compensatory damages, and \$3 million for infringing Suncoast's copyrights drawings. • Former Suncoast employee headed new competitor. Suncoast learned from a client that competitor was using its copyrighted drawings and installation drawings.¹⁷

No.	Trade Secret	Trade Secret Owner	Industry	Conduct and Case Disposition
10	Collection of confidential information regarding executives, companies, and prior search engagements	Kerry/Ford, located in California	Executive Recruiting	• <i>Criminal case</i> • <i>Conviction:</i> California federal jury found a former Kerry/Ford employee guilty of conspiracy to misappropriate trade secrets, and unauthorized receipt, possession, and duplication of trade secrets in violation of 18 U.S.C. § 371.¹⁸ • Sentenced to 12 months and 1 day in prison, and ordered to pay a \$60,000 fine and \$827,983 in restitution.¹⁹ • Note: case is currently on appeal at the Ninth Circuit
11	High frequency trading strategy and infrastructure source code and the data output predictions about investment movements from algorithms analyzing market data	Citadel, LLC, located in Illinois, and "Company A," located in New Jersey	Financial Institution	• <i>Criminal case</i> • <i>Conviction:</i> Former employee pled guilty to unlawful possession and transmission of trade secrets belonging to his former employer in violation of 18 U.S.C. § 1832(a)(2) and (a)(3).²⁰ • Sentenced to 36 months in prison, and ordered to pay \$759,649 in restitution.²¹
12	Computerized customer lists, information, and related notes ²²	Fireworks Spectacular, Inc., and Piedmont Display Fireworks, Inc., both located in Kansas	Fireworks	• <i>Civil case</i> • <i>Disposition:</i> Defendants were acquitted of breach of non-compete agreement and breach of fiduciary duty, but were found guilty of misappropriating trade secrets, specifically Plaintiff's customer information.²³
13	Information regarding gas and oil wells, including seismic data, geological maps, and reserves reports	LexMac Energy LP, and Novus Operating Co. LP, located in North Dakota ²⁴	Gas and Oil	• <i>Civil case</i> • <i>Disposition:</i> 8th Circuit upheld district court's finding that Defendants misappropriated Plaintiffs' trade secrets related to oil and gas wells. Defendants were provided the information as collateral on a loan to lease the wells, but were inappropriately disclosed when Plaintiffs defaulted on the loan.²⁵

No.	Trade Secret	Trade Secret Owner	Industry	Conduct and Case Disposition
14	Market research in the form of PowerPoint presentations on consumer behavior in the greeting cards market. ²⁶	Hallmark Cards Inc., located in Missouri	Greeting cards	• <i>Civil case</i> • <i>Disposition:</i> Jury found defendant corporation guilty of misappropriating plaintiff's trade secrets. Jury awarded \$21.3 million in compensatory damages for the trade secret violation based on an assessment of what defendant would have paid for use of the misappropriated trade secrets. Jury also awarded \$10 million in punitive damages. The jury also found the individual co-defendant guilty and awarded \$125,000 in punitive damages against him.²⁷ • 8th Circuit upheld the award.²⁸
15	Customer information stored in a database allowing for sorting and manipulation. ²⁹	American Family Mutual Insurance Co., located in Wisconsin ³⁰	Insurance	• <i>Civil case</i> • <i>Disposition:</i> parties settled prior to final disposition of the litigation³¹
16	Packaging materials and processes regarding a tamper proof retractable non-reusable syringe. ³²	Retractable Technologies, Inc., located in Texas	Medical Device	• <i>Civil case</i> • <i>Disposition:</i> Jury found defendant corporation guilty of misappropriating plaintiff's trade secrets. Jury awarded \$2,240,640 in compensatory damages for the trade secret violation.³³
17	Information regarding the design and manufacturing of a disposable pen injector. ³⁴	Becton, Dickinson and Company, located in New Jersey	Medical Device	• <i>Criminal case</i> • <i>Conviction:</i> Defendant pled guilty to two counts of theft of trade secrets under 18 U.S.C. § 1832(a)(1), (a)(4). • <i>Disposition:</i> Court ordered the defendant to pay a \$200 fine, \$32,454 in restitution and a sentence of 18 months in prison.³⁵
18	An epoxy-based intumescent fireproofing material used in paint products known as "Chartek"	International Paint, located in Texas and incorporated in Kentucky ³⁶	Paint Industry	• <i>Criminal case</i> • <i>Conviction:</i> Defendant pled guilty to possessing a process formula trade secret formula to produce and/or sell in China under § 1832(a)(3) • <i>Disposition:</i> Sentenced to 12 months and 1 day in prison³⁷

No.	Trade Secret	Trade Secret Owner	Industry	Conduct and Case Disposition
19	Formula for nutritional supplement.	NuScience Corporation, located in California	Nutritional Supplements	• <i>Civil case</i> • <i>Alleged Conduct:</i> Defendants alleged to be using formula that belongs to NuScience. • <i>Disposition:</i> Default judgment entered and NuScience awarded \$600,000, plus \$15,600 in attorneys' fees and \$1,777 in other costs.³⁸ Defendants also take down online statements they know the ingredients and formula for the NuScience's "oxygen + nutrient" supplement.
20	Process for manufacturing chloride-route titanium dioxide, a paint pigment	E.I. DuPont Nemours & Co., headquartered in Delaware, but with plants in the United States, Mexico, and Taiwan	Paint Industry	• <i>Criminal case</i> • <i>Conviction:</i> the main defendant (Liew) was found guilty by a jury of attempt and conspiracy to commit economic espionage under 18 U.S.C. § 1831(a) and of attempt and conspiracy to commit theft of trade secrets and actual possession and conveying of trade secrets under 18 U.S.C. § 1832(a). Liew's co-conspirator (Maergle) was also found guilty by a jury of conspiracy to commit theft of trade secrets and conveying trade secrets under 18 U.S.C. § 1832(a)(2). • <i>Disposition:</i> main defendant sentenced to 180 months in prison and restitution of \$511,487. Other defendants sentenced to 30 months in prison and restitution of \$367,679³⁹
21	Confidential information about "a process for applying hard coatings to the laminate contact surfaces of caul plates." ⁴⁰	Wilsonart International, Inc., located in Michigan	Paint Industry	• <i>Criminal case</i> • <i>Disposition:</i> 6th Circuit affirmed the district court's denial of Defendant's motion to dismiss, finding that the definition of a trade secret under 18 U.S.C. § 1832 was not unconstitutionally vague as to Defendants since Defendant admits he sought to sell information that he knew was proprietary⁴¹

No.	Trade Secret	Trade Secret Owner	Industry	Conduct and Case Disposition
22	Confidential and proprietary information related to the railroad freight business ⁴²	Sierra Railroad Co., located in California	Railroad	• <i>Civil case</i> • <i>Disposition:</i> Jury found railroad company liable for misappropriating plaintiff's trade secrets and awarded \$4.28 M in lost profits and \$18 M in loss of business value, plus \$14.68 M in unjust enrichment, for a total damages award of \$22.282M.⁴³ The confidential information was originally provided in furtherance of an acquisition.⁴⁴ • Note: case is currently on appeal at the Ninth Circuit
23	Semiconductor manufacturing methods	Taiwan Semiconductor Manufacturing (TSMC)	Semiconductor manufacturing	• <i>Civil case</i> • Semiconductor Manufacturing International (SMIC), TSMC's Chinese rival, misappropriated trade secrets—theft occurred in China • Manufacturing technology used in fabricating chips on silicon wafers • <i>Disposition:</i> Following a jury verdict on liability in favor of TSMC, SMIC agreed to pay \$200 million in cash and approximately \$130 million of its company stock.⁴⁵
24	Detailed customer information, including customer product pricing and customer preferences	ATI Industrial Automation, Inc., located in North Carolina	Technology	• <i>Civil case</i> • <i>Disposition:</i> Court granted a joint motion for impoundment and sealing of documents and deposition testimony due to the fact that said materials contained the Plaintiff's trade secrets. The parties ultimately reached an undisclosed settlement agreement.⁴⁶
25	Designs of memory macros for computer chips	UniRAM Technology, Inc., located in California	Technology	• <i>Civil case</i> • <i>Disposition:</i> Jury found defendant corporation guilty of misappropriating the plaintiff company's trade secrets, obtained while consulting for plaintiff as a manufacturing partner. The district court judge entered judgment against defendant, but ultimately the parties settled prior to appeal.⁴⁷

No.	Trade Secret	Trade Secret Owner	Industry	Conduct and Case Disposition
26	Detailed customer information and contractual information	Akamai Technologies, located in Massachusetts	Technology	<i>Criminal case</i> <i>Conviction:</i> Defendant pled guilty to one count of foreign economic espionage under 18 U.S.C. § 1831 for stealing his employer's customer and contractual information and transmitting it to what he thought was, an Israeli agent. <i>Disposition:</i> Sentenced to 1 year imprisonment (6 months in prison and 6 months in home confinement) and a \$25,000 fine.⁴⁸
27	Design and manufacturing processes for computer microprocessors	Transmeta Corporation and Sun Microsystems, both located in California	Technology	<i>Criminal case</i> <i>Conviction:</i> Defendants pled guilty to stealing trade secrets with the intention of benefiting the PRC, in violation of 18 U.S.C. § 1831(a)(2),(3). <i>Disposition:</i> Sentenced to 1 year and 1 day in prison.⁴⁹
28	Source code for proprietary trading strategies and forecasting software ⁵⁰	Quantlab Technologies Ltd., located in Texas	Technology	<i>Civil case</i> <i>Disposition:</i> Court found defendants (a former Quantlab employee and an entrepreneur) liable for misappropriation of trade secrets and conspiracy to misappropriate trade secrets.⁵¹ A jury then determined the appropriate damages award was: \$7.2M against the entrepreneur and \$5M against the employee.⁵² - Note: Defendant's motion for Judgment as a Matter of Law is still pending.
29	Algorithm outlining how to implement a solution to compare different vehicles with differently named features; database schema describing how the data used in the software is arranged ⁵³	Autodata Solutions Company and Autodata Solutions, Inc., located in Texas ⁵⁴	Technology	<i>Civil case</i> <i>Disposition:</i> Jury found that Autodata proved its counterclaim that Versata misappropriated its trade secrets, and awarded \$2 million in damages.⁵⁵

No.	Trade Secret	Trade Secret Owner	Industry	Conduct and Case Disposition
30	(1)technical information re. networkingproducts (e.g.source code; performance capabilities, constraints,and challenges;product developmentplans); (2)customerand marketing information (e.g. customers’unique needs,attitudes, constraints, experiences;terms of agreements; customers’key personnel); (3)employee information (e.g. skilllevels, experience, specialties,attitudes, performance attributes, compensation levels) ⁵⁶	Brocade Communications Systems,Inc.,located in California	Technology	• <i>Civil case</i> • <i>Disposition:</i>Jury found thatA 10 misappropriated Brocade’s trade secrets,butawarded damages of just\$1.00.The jury also found A 10 liable forpatentinfringement, copyrightinfringement,and intentionalinterference with contract.⁵⁷ The parties ultimately agreed to astipulated judgmentfor \$7 5 million.⁵⁸
31	Automated website anti-abuse technology aimed at analyzingdataand shuttingdown abusive websites ⁵⁹	Afilias PLC,located in Dublin Ireland,with subsidiaries located in the US and Canada	Technology	• <i>Civil case</i> • <i>Disposition:</i>Jury found defendant corporation guilty of misappropriatingplaintiff’s trade secrets.Jury awarded \$5 million in compensatory damages forthe trade secretviolation,foratotal award of \$10 million.⁶⁰ • Note:Defendant’s motion for Judgmentas aMatterof Law is still pending

No.	Trade Secret	Trade Secret Owner	Industry	Conduct and Case Disposition
32	Technology “incorporating tunneling magnetoresistance (TMR) into read heads [to] allow for improved storage capacity on hard disk drives.” ⁶¹	Seagate Technology, LLC	Technology	• <i>Civil case</i> • <i>Disposition:</i> Arbitrator found that a former employee and his new employer misappropriated plaintiff’s trade secrets. As a sanction for fabricating evidence of public dissemination of the trade secrets, the arbitrator precluded defendants from disputing the validity of the misappropriation of the trade secrets.⁶² Arbitrator awarded \$525 million in compensatory damages based on the unjust enrichment method, plus approximately \$109 million in pre- and post-judgment interest.⁶³ • The Minnesota Supreme Court upheld the award.⁶⁴
33	Design for computer memory chips	Grail Semiconductor Inc	Technology	• <i>Civil case</i> • <i>Alleged Conduct:</i> Mitsubishi Electric & Electronics USA Inc breached an NDA with Grail. Grail entered into ND A with Mitsubishi to discuss Grail’s designs for small, efficient memory chips in the hopes of getting Mitsubishi to invest. Grail tested new chip launched by Mitsubishi subsidiary and found it contained secret features.⁶⁵ • <i>Disposition:</i> Jury awarded \$124 million. The court ordered a new trial on damages because the award was apparently miscalculated by the jury. The parties settled before the new trial.
34	Price lists, advertising plans, unreleased product attributes	MGA Entertainment, Inc., located in California	Toy (Bratz Dolls)	• <i>Civil case</i> • <i>Alleged Conduct:</i> MGA claims Mattel had an 11-page “how to steal” manual on the trade secrets of competitors. • <i>Disposition:</i> \$8.5M in compensatory and \$8.5M in punitive damages—later vacated by 9th Circuit due to lack of federal jurisdiction. Retried in Cal. State Court seeking \$1B.⁶⁶
35	Wind turbine technology used to regulate the flow of electricity (including proprietary software for the Low Voltage Ride Through system)	AM SC, located in Wisconsin, Massachusetts, and Austria	Wind turbine	• <i>Criminal case</i> • <i>Alleged Conduct:</i> Charges allege a conspiracy to obtain copyrighted information and trade secrets. • <i>Disposition:</i> Case remains pending.⁶⁷

¹ Third Superseding Indictment, *United States v. Li Shaoming*, No.13-CR-00147 (S.D. Iowa Oct.28, 2015)(ECF No.47 9).

² Third Superseding Indictment, *United States v. Li Shaoming*, No.13-CR-00147 (S.D. Iowa Oct.28, 2015)(ECF No.47 9); *see also* Press Release, U.S. Dept. of Justice, Six Chinese Nationals Indicted For Conspiring To Steal Trade Secrets From U.S. Seed Companies (Dec.19, 2013), <http://www.justice.gov/usao-sdia/pr/six-chinese-nationals-indicted-conspiring-steal-trade-secrets-us-seed-companies>.

³ Indictment, at 1, *United States v. Huang*, No.10-CR-0102 (S.D. Ind. June 16, 2010)(Doc 1).

⁴ Sentencing Hearing Transcript, at 17, *United States v. Kexue Huang*, No.10-CR-0102 (S.D. Ind. Dec.22, 2011)(testimony of Dow AgroSciences managing counsel summarizing investigation); Judgment, *United States v. Kexue Huang*, No.10-CR-0102 (S.D. Ind. Mar.6, 2012)(ECF No.107); *see also* Press Release, U.S. Dept. of Justice, Chinese National Sentenced to 8 7 Months in Prison for Economic Espionage and Theft of Trade Secrets (Dec.21, 2011), <http://www.justice.gov/opa/pr/chinese-national-sentenced-8-7-months-prison-economic-espionage-and-theft-trade-secrets>.

⁵ *United States v. Lange*, 312 F.3d 263 (7th Cir.2002)(affirming bench trial conviction); Hearing Minutes, *United States v. Matthew R. Lange*, No.2:99-CR-00174 (E.D. Wis. Mar.2, 2000)(ECF No.34).

⁶ Indictment, *United States v. Shanshan Du & Yu Qin*, No.10-CR-20454 (E.D. Mich. July 22, 2010)(ECF No.3).

⁷ Judgments, *United States v. Shanshan Du & Yu Qin*, No.10-CR-20454 (E.D. Mich. May 9, 2013)(Docs.214, 215); *see also* Press Release, FBI, Two Convicted in Conspiracy to Steal GM Trade Secrets Sentenced to Prison (April 30, 2013), <http://www.fbi.gov/detroit/press-releases/2013/two-convicted-in-conspiracy-to-steal-gm-trade-secrets-sentenced-to-prison>.

⁸ *United States v. Shanshan Du & Yu Qin*, Nos.13-1606, 13-1607, 13-1778, 13-1781 (6th Cir. June 26, 2014) (unpublished), <http://www.ca6.uscourts.gov/opinions.pdf/14a0458n-06.pdf>.

⁹ Plea Agreement, *United States v. Lewis*, No.5:14-CR-00014 (E.D. Ky. Mar.3, 2014)(ECF No.7).

¹⁰ Government's Sentencing Memorandum, *United States v. Lewis*, No.5:14-CR-00014 (E.D. Ky. Oct.8, 2014) (ECF No.19); Judgment (E.D. Ky. Oct.8, 2014)(ECF No.21); *see also* Press Release, U.S. Dept. of Justice, Former Winchester Brake Pad Engineer Pleads Guilty To Theft Of Trade Secrets Charge (March 5, 2014), available at <http://www.justice.gov/usao-edky/pr/former-winchester-brake-pad-engineer-pleads-guilty-theft-trade-secrets-charge>.

¹¹ *United States v. Williams*, 526 F.3d 1312 (11th Cir.2008)(affirming conviction and sentence; concluding "the district court did not err by considering" Coca-Cola's annual revenues "in deciding whether the \$1.5 million intended loss calculated under the guidelines underrepresented the seriousness of the offense"); *see also* Judgment, *United States v. Williams*, No.06-CR-00313-03-JOF (N.D. Ga. May 23, 2007)(ECF No.137).

¹² Judgment, *United States v. Dimson*, No.06-CR-00313-01-JOF (N.D. Ga. May 23, 2007)(ECF No.136).

¹³ Docket Minute Entry, *United States v. Duhaney*, No.06-CR-00313-02-JOF (ND GA June 5, 2007)(ECF No.146).

¹⁴ Order Imposing Criminal Fine, *United States v. Kolon Industries, Inc.*, No.12-CR-00137 (E.D. Va. April 30, 2015)(ECF No.195); Restitution Order (E.D. Va. April 30, 2015)(ECF No.194); Plea agreement at ¶¶ 19-20 (E.D. Va. April 30, 2015)(restitution & fine)(ECF No.191); Judgment (E.D. Va. May 1, 2015)(ECF No.196); *see also* Press Release, U.S. Dept. of Justice, Kolon Industries Inc. Pleads Guilty for Conspiring to Steal DuPont Trade Secrets Involving Kevlar Technology (Apr.30, 2015), <http://www.justice.gov/opa/pr/kolon-industries-inc-pleads-guilty-conspiring-steal-dupont-trade-secrets-involving-kevlar>.

¹⁵ Complaint, *E. I. du Pont de Nemours and Company v. Kolon Industries Inc.*, No.09-CV-00058 (E.D. Va. Feb.3, 2009)(ECF No.1); Dismissal, (E.D. Va. May 27, 2015)(ECF No.3056); *see also* Press Release, DuPont, DuPont and Kolon Settle Trade Secret Litigation (Apr.30, 2015), available at <http://investors.dupont.com/investor-relations/investor-news/investor-news-details/2015/DuPont-and-Kolon-Settle-Trade-Secret-Litigation/default.aspx>.

¹⁶ Plea Agreement, at Factual Basis ¶ 1(C), *United States v. Agodoa*, No. 13-CR-20525 (E.D. Mich. Sept. 25, 2013) (ECF No. 22); Judgment (E.D. Mich. Jan. 17, 2014) (ECF No. 29); *see also* Press Release, U.S. Dept. of Justice, Michigan Man Sentenced For Stealing Trade Secrets (Jan. 16, 2014), available at **Error! Hyperlink reference not valid.** <http://www.justice.gov/usaedmi/pr/michigan-man-sentenced-stealing-trade-secrets>

¹⁷ *Suncoast Post-Tension Ltd. v. Scoppa et al.*, No. 4:13-cv-03125 (S.D. Tex. 2015).

¹⁸ Amended Judgment, *United States v. Nosal*, No. 08-cr-00237-EMC (N.D. Cal. May 30, 2014) (ECF No. 552); Second Superseding Indictment, *United States v. Nosal*, No. 08-cr-00237-EMC (N.D. Cal. Feb. 28, 2013) (ECF No. 309).

¹⁹ Amended Judgment, *United States v. Nosal*, No. 08-cr-00237-EMC (N.D. Cal. May 30, 2014) (ECF No. 552); *see* appeal information at No. 14-10037 (9th Cir. 2015) and No. 14-10275 (9th Cir. 2015).

²⁰ Plea Agreement, *United States v. Pu*, No. 11-cr-00699 (N.D. Ill. Aug. 7, 2014) (ECF No. 175).

²¹ Judgment, *United States v. Pu*, No. 11-cr-00699 (N.D. Ill. Jan. 15, 2015) (ECF No. 206).

²² *Fireworks Spectacular, Inc. v. Premier Pyrotechnics, Inc.*, 147 F. Supp.2d 1057 (D. Kan. May 17, 2001).

²³ *Id.*

²⁴ Judgment, *LexMac Energy, L.P. v. Macquarie Bank Ltd.*, No. 4:08-CV-00048 (D. N.D. Jan. 7, 2014) (ECF No. 333).

²⁵ *Macquarie Bank Limited v. Bradley D. Knickel et al.*, No. 14-1684 (8th Cir. July 17, 2015).

²⁶ *Hallmark Cards, Inc. v. Monitor Clipper Partners, LLC*, No. 13-1905 (8th Cir. July 15, 2014).

²⁷ Jury Verdict Form, *Hallmark Cards, Inc. v. Monitor Clipper Partners, LLC*, No. 08-cv-00840 (W.D. Mich., Nov. 19, 2012) (ECF No. 527); *see also* Judgment, *Hallmark Cards, Inc. v. Monitor Clipper Partners, LLC*, No. 08-cv-00840 (W.D. Mich., Nov. 20, 2012) (ECF No. 526); Judgment, *Hallmark Cards, Inc. v. Monitor Clipper Partners, LLC*, No. 08-cv-00840 (W.D. Mich., Mar. 20, 2013) (ECF No. 588).

²⁸ Judgment, *Hallmark Cards, Inc. v. Monitor Clipper Partners, LLC*, No. 13-1905 (8th Cir. July 15, 2014).

²⁹ *Am. Family Mut. Ins. Co. v. Roth*, 485 F.3d 930 (7th Cir. May 7, 2007).

³⁰ Complaint at 2, *Am. Family Mut. Ins. Co. v. Roth*, No. 05-cv-03839 (N.D. Ill. June 30, 2005), ECF No. 1.

³¹ Notification of Docket Entry, *Am. Family Mut. Ins. Co. v. Roth*, No. 05-cv-03839 (N.D. Ill. Jan. 31, 2011), ECF No. 400.

³² Amended Complaint, *Retractable Techs., Inc. vs. Occupational & Med. Innovations, Ltd.*, No. 08-cv-00120 (E.D. Tex. May 13, 2009), ECF No. 84; Order Denying Defendant's Judgment as a Matter of Law, *Retractable Techs., Inc. vs. Occupational & Med. Innovations, Ltd.*, No. 08-cv-00120 (E.D. Tex. Aug. 11, 2010), ECF No. 268.

³³ Jury Verdict Form, *Retractable Techs., Inc. vs. Occupational & Med. Innovations, Ltd.*, No. 08-cv-00120 (E.D. Tex. Dec. 18, 2009), ECF No. 228; Order Denying Defendant's Judgment as a Matter of Law, *Retractable Techs., Inc. vs. Occupational & Med. Innovations, Ltd.*, No. 08-cv-00120 (E.D. Tex. Aug. 11, 2010), ECF No. 268.

³⁴ Complaint, *United States v. Maniar*, No. 13-CR-06085 (D. N.J. June 4, 2013), ECF No. 1.

³⁵ Plea Agreement, *United States v. Maniar*, No. 13-CR-06085 (D. N.J. May 28, 2014), ECF No. 22; Judgment, *United States v. Maniar*, No. 13-CR-06085 (D. N.J. Oct. 16, 2014), ECF No. 27.

³⁶ Indictment, *United States v. Zeng*, No. 08-CR-00075 (S.D. Tex. Jan. 22, 2008), ECF No. 1.

³⁷ Plea Agreement, *United States v. Zeng*, No. 08-CR-00075 (S.D. Tex. May 16, 2008), ECF No. 30; Judgment, *United States v. Zeng*, No. 08-CR-00075 (S.D. Tex. May 22, 2008), ECF No. 33; *see also* Press Release, U.S. Dept. of Justice, Chinese Chemist Convicted In Theft Of Trade Secrets (May 16, 2008), <http://www.justice.gov/archive/criminal/cybercrime/press-releases/2008/zengConvict.pdf>.

³⁸ *NuScience Corp. v. Henkel*, No. 2:08-cv-02661 (C.D. Cal. 2009).

³⁹ Judgment, *United States v. Liew*, No.11-CR-00573 (N.D. Cal. Aug. 28, 2014), ECF No.921; Judgment, *United States v. Liew*, No.11-CR-00573 (N.D. Cal. Sep. 2, 2014), ECF No.924; *see also* Press Release, U.S. Dep't of Justice, Walter Liew Sentenced to 15 Years in Prison for Economic Espionage (July 11, 2014), <http://www.justice.gov/usao-ndca/pr/walter-liew-sentenced-fifteen-years-prison-economic-espionage>.

⁴⁰ *United States v. Krumrei*, 258 F.3d 535, 536 (6th Cir. 2001).

⁴¹ *Id.* at 539.

⁴² Counterclaim, *Patriot Rail Corp. v. Sierra R.R. Co.*, No.09-CV-00009 (E.D. Cal. Apr. 2, 2010), ECF No.65, *appeal docketed*, No.15-16587 (9th Cir. Aug. 7, 2015).

⁴³ Jury Verdict, *Patriot Rail Corp. v. Sierra R.R. Co.*, No.09-CV-00009 (E.D. Cal. Mar. 28, 2014), ECF No.447, *appeal docketed*, No.15-16587 (9th Cir. Aug. 7, 2015); *see also* Entry of Judgment, *Patriot Rail Corp. v. Sierra Railroad Co.*, No.09-CV-00009 (E.D. Cal. Oct. 31, 2014), ECF No.532, *appeal docketed*, No.15-16587 (9th Cir. Aug. 7, 2015).

⁴⁴ Counterclaim, *Patriot Rail Corp. v. Sierra R.R. Co.*, No.09-CV-00009 (E.D. Cal.), ECF No.65, *appeal docketed*, No.15-16587 (9th Cir. Aug. 7, 2015).

⁴⁵ *TSMC N. Am. et al. v. SMIC Ams. et al.*, No.RG06-28 6111 (Cal. Super. Ct. Alameda County).

⁴⁶ Order Sealing Documents at 15–16, *ATI Indus. Automation, Inc. v. Applied Robotics, Inc.*, No.09-CV-00471 (July 12, 2011), ECF No.84.

⁴⁷ Entry of Judgment, *UniRAM Tech., Inc. v. Taiwan Semiconductor Mfg. Co.*, No.04-CV-01268 (N.D. Cal. Apr. 17, 2008) (ECF No.628).

⁴⁸ Plea Agreement, *United States v. Elliot Doxer*, No.111-CR-10268 (D. Mass. July 20, 2011) (ECF No.19); Sentencing Hearing Transcript at 5–8, 9–10, 15 (D. Mass. Dec. 21, 2011) (ECF No.29); *see also* Press Release, U.S. Dep't of Justice, Employee of High Technology Company Charged with Seeking to Provide Confidential Business Information to a Foreign Government (Oct. 6, 2010), *available at* <http://www.justice.gov/archive/usao/ma/news/2010/October/DoxerElliotPR.html>.

⁴⁹ Judgment, *United States v. Fei Ye, et al.*, No.02-CR-20145 (N.D. Cal. Nov. 25, 2008) (ECF No.268); Judgment, *United States v. Fiy Ye, et al.*, No.02-CR-20145 (N.D. Cal. Nov. 25, 2008) (ECF No.270); *see also* Press Release, U.S. Dep't of Justice, Two Men Plead Guilty to Stealing Trade Secrets from Silicon Valley Companies to Benefit China (Dec. 14, 2006), *available at* <http://www.justice.gov/archive/criminal/cybercrime/press-releases/2006/yePlea.htm>.

⁵⁰ Complaint, *Quantlab Technologies Ltd. v. Godlevsky, et al.*, No.4:09-CV-04039 (S.D. Tex. Dec. 18, 2009) (ECF No.1); *see also* Third Amended Complaint, *Quantlab Technologies Ltd. v. Godlevsky, et al.*, No.:09-CV-04039 (S.D. Tex. July 21, 2014) (ECF No.533).

⁵¹ Order, *Quantlab Technologies Ltd. v. Godlevsky, et al.*, No.04-CV-04039 (S.D. Tex. July 21, 2014) (ECF No. 725).

⁵² Jury Verdict, *Quantlab Technologies Ltd. v. Godlevsky, et al.*, No.14-CV-04039 (S.D. Tex. May 20, 2015) (ECF No.761); *see also* Quantlab's Motion for Entry of Final Judgment, *Quantlab Technologies Ltd. v. Godlevsky, et al.*, No.04-CV-04039 (S.D. Tex. July 2, 2015) (ECF No.786).

⁵³ Memorandum Opinion and Order, *Versata Software, Inc. v. Internet Brands, Inc.*, No.08-CV-00313 (E.D. Tex. Oct. 9, 2012) (ECF No.371).

⁵⁴ Complaint, *Versata Software, Inc. v. Internet Brands, Inc.*, No.08-CV-00313 (E.D. Tex. Aug. 8, 2008) (ECF No.1).

⁵⁵ Memorandum Opinion and Order, *Versata Software, Inc. v. Internet Brands, Inc.*, No.08-CV-00313 (E.D. Tex. Oct. 9, 2012) (ECF No.371).

⁵⁶ Third Amended Complaint, *Brocade Communications Systems, Inc. v. A10 Networks, Inc.*, No.10-CV-03428 (N.D. Cal. Apr. 29, 2011) (ECF No.85).

⁵⁷ Jury Verdict, *Brocade Communications Systems, Inc. v. A10 Networks, Inc.*, No.10-CV-03428 (N.D. Cal. Aug. 6, 2012) (ECF No. 771).

⁵⁸ Stipulated Final Judgment, *Brocade Communications Systems, Inc. v. A10 Networks, Inc.*, No.10-CV-03428 (N.D. Cal. June 7, 2013) (ECF No. 1026).

⁵⁹ Complaint, *Afilias PLC v. Architelos, Inc.*, 15-cv-00014 (E.D. Va. Jan. 5, 2015) (ECF No. 1).

⁶⁰ Jury Verdict, *Afilias PLC v. Architelos, Inc.*, 15-cv-00014 (E.D. Va. Aug. 24, 2015) (ECF No. 240).

⁶¹ Further details regarding the specific trade secrets were not made public. *Seagate Technology, LLC v. Western Digital Corp.*, 854 N.W.2d 750, 754 (Minn. 2014).

⁶² *Seagate Technology, LLC v. Western Digital Corp.*, 854 N.W.2d 750, 754-56 (Minn. 2014).

⁶³ *Seagate Technology, LLC v. Western Digital Corp.*, 834 N.W.2d 555, 559 (Minn. Ct. App. 2013).

⁶⁴ *Seagate Technology, LLC v. Western Digital Corp.*, 854 N.W.2d 750, 767 (Minn. 2014).

⁶⁵ *Grail Semiconductor Inc. v. Mitsubishi Electric & Electronics USA Inc. et al.*, No. 1-07-CV-098590 (C al. Sup. Ct. July 24, 2012).

⁶⁶ Complaint, *MGA Entertainment, Inc. v. Mattel, Inc.*, No. B C532708, (C al. Sup. Ct. Jan. 13, 2014) (Complaint for Trade Secret Misappropriation).

⁶⁷ Indictment, *United States v. Sinovel Wind Group Co., Ltd., et al.*, No. 13-CR-84 (W.D. Wis. June 27, 2013) (ECF No. 25); see also Press Release, U.S. Dept. of Justice, Sinovel Corporation and Three Individuals Charged in Wisconsin with Theft of Amsc Trade Secrets (June 27, 2013), <http://www.justice.gov/opa/pr/sinovel-corporation-and-three-individuals-charged-wisconsin-theft-amsc-trade-secrets>.

Appendix C

Military Application Trade Secret Examples

Based on Recent Criminal and Civil Cases

Appendix C
Military Application Trade Secret Examples
Based on Recent Criminal and Civil Cases

No.	Military Application Trade Secret	Trade Secret Owner	Conduct and Case Disposition
1	Visual simulation source code and software for military aircraft training	Quantum3D, located in California	• <i>Criminal case</i> • <i>Conviction:</i> Defendant pled guilty to foreign economic espionage under 18 U.S.C. § 1831(a)(3) for possessing a stolen trade secret with the intent to benefit a foreign government, and for violating the Arms Export Control Act under 22 U.S.C. §§ 2778(b)(2), 2778(c) for exporting a defense article without obtaining a license to do so by the Department of State • <i>Disposition:</i> Defendant sentenced to 24 months and one day in prison and \$10,200 fine¹
2	Phased array antenna project for the space shuttle and two documents concerning the Delta IV Rocket, a booster rocket designed to launch manned space vehicles	Rockwell International and Boeing, located in California	• <i>Criminal case</i> • <i>Conviction:</i> Former Rockwell International and Boeing engineer convicted in a bench trial on six counts of foreign economic espionage under 18 U.S.C. §§ 1831(a)(3), as well as one count of conspiring to commit economic espionage, one count of acting as an unregistered foreign agent, and one count of making a false statement to federal agents • <i>Disposition:</i> Sentenced to serve 188 months in prison²
3	Designs, mechanical parts and hardware for the manufacture and testing of detector logarithmic video amplifiers and successive detection logarithmic video amplifiers, which are microwave technology components used to enhance navigation, radar jamming, and locating enemy signals during warfare ³	Genesis Microwave, Inc., located in California	• <i>Criminal case</i> • <i>Conviction:</i> Defendant pled guilty to stealing, downloading, and possessing trade secret under 18 U.S.C. § 1832 • <i>Disposition:</i> Defendant sentenced to 24 months in prison and ordered to pay \$15,000 in restitution⁴⁵

4	A systems architecture document (a teaching instrument) for an iDEN cellular communication network, a white paper analyzing features for said network, and an interface control document to catalog messages used between network elements. ⁶	Motorola, based in Illinois	• <i>Criminal case</i> • <i>Conviction:</i> Defendant was convicted in a bench trial on three trade secret counts under 18 U.S.C. § 1832 for stealing, downloading, and possessing trade secrets from her employer, but was acquitted on the three charges under 18 U.S.C. § 1831 due to reasonable doubt that she intended to benefit the PRC in any way • <i>Disposition:</i> Defendant sentenced to 48 months in prison and ordered to pay \$20,000 fine⁷
5	\$2 billion worth of trade technical details and manuals related to the F-35 Joint Strike Fighter program and its engines and other military jet engines. U.S. Customs and Border Control officials discovered the documents in California in 11 crates bound for Iran. ⁸	Multiple defense contractors, including Pratt & Whitney and Rolls Royce	• <i>Criminal case</i> • <i>Conviction:</i> Defendant pleaded guilty to one count of unlawful export and attempted export of defense articles from the U.S. in violation of the Arms Export Control Act. • <i>Disposition:</i> Defendant sentenced to 97 months in prison and ordered to pay \$50,000 fine⁹

¹ Redacted Plea Agreement, *United States v. Meng*, No. 04-CR-20216-JF (N.D. Cal. Aug. 1, 2007) (ECF No. 76); Judgment (N.D. Cal. June 24, 2008) (ECF No. 103); *see also* Press Release, U.S. Dep't of Justice, Former Chinese National Convicted of Economic Espionage to Benefit China Navy Research Center (Aug. 2, 2007), http://www.justice.gov/archive/opa/pr/2007/August/07_nsd_572.html.

² *United States v. Chung*, 633 F. Supp. 2d 1134 (C.D. Cal. 2009) (Memorandum of Decision), *aff'd*, 659 F.3d 815 (9th Cir. 2011) (affirming conviction and sentence); Judgment, *United States v. Chung*, No. 8:08-CR-00024 (C.D. Cal. Feb. 11, 2010) (ECF No. 172); *see also* Press Release, U.S. Dep't of Justice, Former Boeing Engineer Sentenced To Nearly 16 Years In Prison For Stealing Aerospace Secrets For China (Feb. 8, 2010), <http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2012/03/15/chungSent.pdf>.

³ Plea Agreement Factual Basis for Plea, *United States v. Cotten*, No. 08-CR-00042-EJG (E.D. Cal. Feb. 29, 2008) (ECF No. 9).

⁴ Plea Agreement, *United States v. Cotten*, No. 2:08-CR-00042-EJG (E.D. Cal. Feb. 29, 2008) (ECF No. 9); Judgment, *United States v. Cotten*, No. 08-CR-00042-EJG (EDCA May 21, 2008) (ECF No. 13).

⁶ *United States v. Jin*, 833 F. Supp. 2d 977, 995-998 (N.D. Ill. 2012).

⁷ *Id.* at 977; *United States v. Jin*, 733 F.3d 718, 718 (7th Cir. 2013).

⁸ Affidavit to Complaint, *United States v. Khazaei*, No. 3:14-cr-00009 (D. Conn. 2015) (ECF No. 1).

⁹ Judgment, *United States v. Khazaei*, No. 3:14-cr-00009 (D. Conn. 2015) (ECF No. 89).



December 1, 2015

Hon. Chuck Grassley
United States Senate
135 Hart Senate Office Building
Washington, D.C. 20510

Hon. Patrick Leahy
United States Senate
437 Russell Senate Building
Washington, D.C. 20510

Dear Chairman Grassley and Ranking Member Leahy,

Thank you for your leadership on the Defend Trade Secrets Act of 2015 (S. 1890) and for holding a hearing on December 2nd to discuss this vital issue. The National Alliance for Jobs and Innovation (NAJI) strongly supports this important legislation.

I am NAJI's President and also the former Attorney General of Washington State and former President of the National Association of Attorneys General. NAJI represents over 400 small and medium-size manufacturing and high-tech enterprises around the United States for which trade secrets are essential to success. In fact, the 2015 NAJI Annual Member Survey revealed that for our members, trade secrets are the most important form of IP – *74% of IP-users cited trade secrets as important to their business success, followed by 67% for patents and 58% and 33% for trademarks and copyrights, respectively.*

Trade secrets take many forms – such as manufacturing processes, industrial techniques, customer lists, and product formulas – but share one common feature: their protection is critical for the competitiveness of companies that are creating American jobs.

The know-how these trade secrets embody can take years to develop, representing some of the best of American ingenuity. NAJI members have worked hard and invested a huge amount of resources to develop this proprietary knowledge, and it must be secured if American companies are to maintain our nation's position at the pinnacle of innovation and competitiveness.

Our members' trade secrets are under attack at every turn from industrial espionage, both domestic and foreign. Competitors looking to gain an unfair advantage by stealing know-how rather than engaging in expensive research and development are targeting our trade secrets. This theft harms our global competitiveness, our innovation, and the jobs we contribute to the U.S. economy. The threat is all too real: broad industry surveys have found that as many as 60 percent of companies report attempted or actual trade secret theft in a given year.

In the 21st Century, trade secret theft is no longer limited to when a competitor steals customer lists or other information from a company across the street or across town. It is now a national and international epidemic. The Defend Trade Secrets Act of 2015 would create a federal civil cause of action for trade secret misappropriation. Trade secret owners would continue to rely on the traditional state law of trade secrets while benefiting from significantly strengthened trade secret protection under the Act. This much-needed legislation would give American small businesses the ability to pursue fast action in a single court, which will often prove the more efficient forum when the threat is interstate and involves actions that cross jurisdictional boundaries.

Moreover, a new statutory option to seek relief in federal court will not increase litigation, but rather will simply shift litigation to a different forum. Indeed, in cases where a company currently must seek relief in multiple state courts, having access to federal court should reduce litigation overall and reduce total costs to the harmed company without changing the substantive state law of trade secrets.

Hon. Chuck Grassley
Hon. Patrick Leahy

December 1, 2015

The future innovation that American businesses and American workers are depending on for economic success relies in significant part on strong trade secret protection. We must safeguard America's trade secrets, and the millions of jobs that depend on them, with legislation that provides trade secret owners with a federal civil right of action – the same right that is already afforded to patent, trademark and copyright owners.

We look forward to working with you and the entire Congress to see the Defend Trade Secrets Act enacted this year.

Sincerely,

A handwritten signature in black ink that reads "Rob McKenna". The signature is written in a cursive, flowing style.

Rob McKenna, President
National Alliance for Jobs and Innovation

December 2, 2015

The Honorable Orrin Hatch
United States Senator
104 Hart Senate Office Building
Washington, DC 20510

The Honorable Christopher Coons
United States Senator
172A Russell Senate Office Building
Washington, DC 20510

The Honorable Jeff Flake
United States Senator
413 Russell Senate Office Building
Washington, DC 20510

Dear Senator Hatch, Senator Coons, and Senator Flake:

The undersigned companies and organizations write to express our support for the Defend Trade Secrets Act of 2015. We appreciate your leadership on this issue.

The Defend Trade Secrets Act will create a harmonized, uniform standard and system for companies to protect their trade secrets. Your bipartisan legislation will establish a strong standard for trade secret protection.

Trade secrets are an essential form of intellectual property. Trade secrets include information as broad-ranging as manufacturing processes, product development, industrial techniques, formulas, and customer lists. The protection of this form of intellectual property is critical to driving the innovation and creativity at the heart of the American economy. Companies in America, however, are increasingly the targets of sophisticated efforts to steal proprietary information, harming our global competitiveness.

Existing state trade secret laws are inadequate to address the interstate and international nature of trade secret theft today. Federal law protects trade secrets through the Economic Espionage Act of 1996 (“EEA”), which provides criminal sanctions for trade secret misappropriation. While the EEA is a critical tool for law enforcement to protect the clear theft of our intellectual property, U.S. trade secret owners also need access to a federal civil remedy and the full spectrum of legal options available to owners of other forms of intellectual property, such as patents, trademarks, and copyrights.

The Defend Trade Secrets Act will create a federal remedy that will provide a consistent, harmonized legal framework and help avoid the commercial injury and loss of employment that can occur when trade secrets are stolen. We are proud to support it.

The Honorable Orrin Hatch
The Honorable Christopher Coons
The Honorable Jeff Flake
December 2, 2015
Page 2

Sincerely,

Adobe
AdvaMed
Alliance of Automobile Manufacturers
American Intellectual Property Law Ass'n
Association of Global Automakers, Inc.
Biotechnology Industry Organization (BIO)
The Boeing Company
Boston Scientific
BSA | The Software Alliance (BSA)
Caterpillar Inc.
Corning Incorporated
The Dow Chemical Company
DuPont
Eli Lilly and Company
General Electric
Honda
IBM
Illinois Tool Works Inc.
Information Technology Industry Council (ITI)
Intel
International Fragrance Association, North America
Internet Commerce Coalition
Johnson & Johnson
Medical Device Manufacturers Association (MDMA)
Medtronic
Michelin North America
Micron
Microsoft
Monsanto
National Alliance for Jobs and Innovation (NAJI)
National Association of Manufacturers (NAM)
The New England Council
NIKE

The Honorable Orrin Hatch
The Honorable Christopher Coons
The Honorable Jeff Flake
December 2, 2015
Page 2

Pfizer
Philips
The Procter & Gamble Company
SAS
Semiconductor Industry Association (SIA)
Siemens Corporation
Software & Information Industry Association (SIIA)
U.S. Chamber of Commerce
United Technologies Corporation
3M

cc: Chairman Charles E. Grassley, Senate Judiciary Committee
Ranking Member Patrick J. Leahy, Senate Judiciary Committee
Members of the Senate Judiciary Committee

How Trade Secrets Are Helping Foster Cloud Innovation

by Jule Sigall, Assistant General Counsel, Intellectual Property Group
Microsoft Corporation

On Wednesday, the Senate Judiciary Committee will hold an important hearing on protecting trade secrets. We applaud the Committee for convening this hearing and urge that it soon consider the Defend Trade Secrets Act (S. 1890), bipartisan legislation that would create a uniform, federal standard for trade secret protection and responds to the nature of 21st Century innovation.

Trade secrets have long been a popular means of protecting innovation among traditional industries. Secret formulas, customer lists, and methods of manufacturing have produced value to companies that have taken the necessary steps to ensure their confidentiality.

Trade secrets are still critical today, especially for technology companies, big and small. Consider Microsoft's Cortana, for example, which is our personal digital assistant. True – she can help you make calls, send texts, set and remind you of meetings, and give you directions to your next appointment. But behind Cortana sits a vast amount of technology developed or enhanced in-house by Microsoft – voice recognition; language translation; reactive and predictive algorithms that can synthesize context, location, and data, and interface with the vast resources of the Bing search engine index; and a complex array of cloud servers to crunch and serve data in real time. This technology represents tens of thousands of hours of research, trial and error, and continued improvement as Cortana is adapted for new devices and new scenarios.

Certainly patent and copyright provide protection for some of this innovation, but trade secret protection is vital for something like Cortana that continues to innovate. Many important, but unseen aspects of products – the “know-how” – are trade secrets: the product development process, the business plan around how and when the product will be unveiled, future improvements, and plans for adapting such technology into entirely new product categories.

These aspects may hold significantly more value as trade secrets because they cannot be easily discovered by competitors without making similar substantial investments in research and development. This form of acquired know-how is often the competitive edge that companies need to succeed – and what makes them unique in crowded and competitive marketplaces. For that reason, trade secrets contribute significantly to the value of technology companies, especially startups that have yet to develop extensive intellectual property portfolios. Protecting the value of such innovation is a way of incentivizing further research and development that continually improves the services we can provide customers.

As our economy and our manufacturing processes have rapidly shifted to embrace cloud-powered technologies and services, the relevance of trade secret protection has only increased. Businesses no longer compete just against the company across the street – they sell products and services around the country and around the world. A decade ago a small business might have written its know-how on paper – its business plans, its manufacturing process, the secret sauce that give the business a competitive edge – and locked it in a desk drawer or a safe. Today, companies rely on networks of manufacturers and service providers accessing, storing, and using their trade secrets in many locations, and their ability to share secrets with such providers, with

the knowledge they will remain protected, remains vital to the growth of cloud-powered economies.

A trade secret is unique among forms of intellectual property in how it is legally protected. While it is a *federal* crime to steal a trade secret, a business that has its trade secrets stolen must rely on *state* law to pursue a civil remedy. Owners of copyrights, patents, and trademarks can go to federal court to protect their property and seek damages when their property has been infringed, but trade secret owners do not have access to such a federal remedy.

Our state-by-state system for trade secret protection was simply not built with the digital world in mind. In today's global economy, however, trade secrets are increasingly stored and used across state lines and even national borders. A uniform, national standard for protection will greatly benefit businesses of all sizes.

Microsoft commends Chairman Grassley and Ranking Member Leahy for convening today's hearing, and applauds the leadership of Senators Hatch and Coons and Representatives Collins, Nadler, Holding and Jeffries in introducing the Defend Trade Secrets Act, legislation that Microsoft is pleased to support. We look forward to working with these leaders and others as Congress considers this important legislation.

Time to Reform the Computer Fraud and Abuse Act

By Mark L. Krotoski

November 18, 2015- An essential aspect of any effective cybersecurity strategy is the ability to obtain meaningful remedies and enforcement for the theft of data when possible. Yet federal law has proven inadequate over the past several years to address current challenges involving the theft of data from a computer.

The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. §§ 1030, the primary federal statute to address criminal and civil computer violations, was originally enacted in 1984 and has been amended nine times, the last time in 2008. The CFAA has separate provisions to address different computer offenses including hacking (Section 1030(a)(5)); extortion (Section 1030(a)(7)); obtaining information from a financial institution, federal agency or protected computer (Section 1030(a)(2)); and computer fraud (Section 1030(a)(4)), among other provisions.

The CFAA has not kept up with changes in technology and fails to address many common scenarios involving efforts to steal data by insiders, former insiders and outsiders. Given the importance of cybersecurity and the role and protection of data in our economy today, Congress needs to modernize and strengthen the primary federal computer statute to address the variety of ways in which data may be stolen.

Current 'Nosal' Case

The latest reminder on the need for Congress to update and clarify the statute was highlighted in the recent Oct. 20, 2015 Ninth Circuit oral argument in *United States v. David Nosal*, No. 14-10037. The case involved defendant Nosal's role with others in downloading trade secrets and other proprietary information from the confidential database of his former employer, Korn/Ferry International.

At a jury trial, defendant Nosal was convicted as charged on six counts: one conspiracy count, three CFAA counts for computer fraud under 18 U.S.C. §§ 1030(a)(4) and 2, and two trade secret counts. He was sentenced to serve a year and a day in prison, pay a \$60,000 fine and \$827,983.25 in restitution.

One central issue now pending on appeal concerns the application and scope of the CFAA. Under prevailing Ninth Circuit case law, on the three Section 1030(a)(4) computer fraud counts, the government was required to establish that the defendant aided and abetted the (1) access of a protected computer, (2) "without authorization" or "exceed[ing] authorized access," (3) knowingly and with intent to defraud, and thereby (4) furthered the intended fraud and obtained something of value. See *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1132 (9th Cir. 2009). The dispute in the appeal focuses on the second element.

Over the past several years, the courts have wrestled with the meaning of "without authorization" and "exceeding authorized access." These statutory terms have generated confusion concerning the scope of the CFAA in a variety of circumstances most often arising in the employee or former employee context.

In Nosal, the defendant was a top executive and Silicon Valley managing director of Korn/Ferry International, a leading executive-search firm. After departing the company in 2004, Nosal began his own employment search company. Two other employees, who joined him in 2005, persuaded a current employee to share her password to give them access to the confidential database which they used to run searches and obtain source lists, names and information for employment candidates in Nosal's new firm.

It is undisputed that Nosal and the two former employees lacked authority to directly access the specific information they sought from the confidential database of their former employer. The government argues that the two former employees, aided and abetted by Nosal, accessed the company computers "without authorization" since all of their access rights had been rescinded. Instead, they used the password credentials of a current employee to obtain the information from the confidential database. The company policy prohibited the employee from sharing her log-in credentials. In contrast, the defense contends on appeal that "the downloads in question were effectuated by the consensual use of a password validly issued to a KFI employee, and thus involved no hacking."

During the oral argument, Ninth Circuit Judge M. Margaret McKeown asked whether the former employees were essentially "going through the backdoor to get what they cannot get through the front door" since they were no longer employees at the company and their authorization had been revoked. Ninth Circuit Judge Stephen Reinhardt noted that there was no disagreement on these facts. In his view, the question was whether a crime resulted under the present authorization language of the CFAA when someone else shared their password for access. Chief Judge Sidney R. Thomas wondered how the statute would apply if, as urged by the defense, the password was obtained by phishing or the employee was duped into providing the password. Judge McKeown also asked "who has the authority to give authorization?"

According to the defense, "password sharing is not hacking" and does not violate the CFAA. The defense asserts that "it is not merely the computer owner who can confer authorization—it is also the password holder."

This hyper-technical view relies on the "authorization" terms of the statute to claim that the shared password by a current employee granted "permission" to the two former employees whose authorization to access the company network had been rescinded. Under this position, any employee can provide authorization or access to outsiders even when the company policy forbids the sharing of passwords or access. This result would empower any employee to override clear company policy. Defendants could use this approach as an exception to evade enforcement under the statute. Also, if social engineering is used to entice someone to share their log-in credential, the access would be "authorized" under this construction. The outcome should not turn on the role or status of the person supplying the access credentials.

As noted during the oral argument, neither the government nor defense is asking the court to adopt a bright line rule that the sharing of a password always falls within or outside the CFAA. Given the narrow set of circumstances, the decision should be based on a fact specific inquiry on whether sufficient evidence was presented at trial to sustain the three CFAA jury convictions. The recent oral argument shows how some basic facts concerning a scheme to steal data can get unnecessarily bollixed around whether the conduct was "authorized" or not by one employee.

Inconsistent Application of the CFAA

But the problems with the CFAA extend beyond the Nosal oral argument. Over the past several years, a significant split in the circuit courts has emerged over the scope and application of the CFAA. The result is that the same or similar conduct is treated differently depending on where the theft occurred.

Generally, two judicial groups have emerged in applying the statute. The First, Fifth, Seventh and Eleventh Circuits apply the statute more broadly allowing for remedies or enforcement based on the theft or destruction of data by current or former employees. (See *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001); *United States v. John*, 597 F.3d 263, 269 (5th Cir. 2010); *International Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006); *United States v. Rodriguez*, 628 F.3d 1258, 1260 (11th Cir. 2010).) The broader construction group considers whether the conduct involves a breach of a duty of loyalty or a non-business purpose or is contrary to non-disclosure or use terms.

In contrast, two circuits apply the CFAA more narrowly: the Fourth and Ninth Circuits. (See *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 202 (4th Cir. 2012); *Brekka*, 581 F.3d at 1129-30, 1134-35; *United States v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012) (en banc).) These two courts focus on whether the original authorized access to the network was restricted or has been rescinded.

Given the importance of protecting computer data against theft by insiders and outsiders, this inconsistent application is simply intolerable. Congress should resolve the uncertain and confusing application of the CFAA by the courts and clarify that the theft of data, by any means, will be subject to effective civil remedies and criminal enforcement.

Congressional Reform Options

The Nosal case is just the latest reminder on the need for Congress to modernize and strengthen the CFAA. There are some distinct legislative options Congress can consider.

First, Congress can substitute a new standard which does not rely on "authorization" but instead focuses on the "use" or "purpose" to misuse the information. Several courts have considered this approach.

Second, Congress can use a misappropriation standard which would focus on whether the information was misappropriated or stolen. Initial authorized or unauthorized access to the information would not be dispositive. Instead, the facts concerning the intent and circumstances of the theft would determine whether the statute was violated.

Finally, if Congress is determined to retain the "authorization" standard, Congress should redefine the terms "without authorization" and "exceeds authorized access" to clarify that the statute applies when initial permitted access to information is later rescinded or abused. The current lack of clear guidance has resulted in disparate standards developed by the courts.

Congress should also consider establishing separate standards and provisions for civil cases. In 1994, Congress added a civil private right of action to the criminal statute. Consequently, some of the same provisions may result in civil or criminal enforcement. Consequently, the statute does not recognize common distinctions in proof for civil and criminal provisions. Traditionally, criminal cases have a higher standard for intent, such as an intent to defraud. Additionally, Congress should extend the two-year statute of limitations to five years, comparable to the criminal provisions.

The bottom line is that the theft of data should be subject to criminal penalties and civil remedies regardless of whether it is committed by insiders, former insiders, or outsiders. The outcome should not turn on some hyper-technical application on whether initial access was "authorized" or "exceeded." Theft of data is quite simply theft. As in other contexts, a jury can decide whether a theft occurred by considering the defendant's intent and all of the relevant circumstances and facts. These inquiries are fact-specific. The current CFAA should be updated to address the cyber realities of today including threats from insiders and outsiders. It is time for Congress to strengthen and modernize the CFAA.

Mark Krotoski is a partner in the litigation, privacy and cybersecurity, and antitrust practice groups of Morgan, Lewis & Bockius, resident in the Silicon Valley office. He previously served as the National Coordinator of the Computer Hacking and Intellectual Property Program (CHIP) in the Criminal Division of the U.S. Department of Justice and as a CHIP prosecutor in Silicon Valley prosecuting a range of computer intrusions, computer crimes, and economic espionage and trade secret cases. The views of the author do not necessarily represent those of the firm or its clients.

Link to article on Therecorder.com:

<http://www.therecorder.com/home/id=1202742832060/Viewpoint-Time-to-Reform-the-Computer-Fraud-and-Abuse-Act?slreturn=20151030151714>

Reprinted with permission from the November 18, 2015 edition of The Recorder© 2015 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. ALMReprints.com – 877-257-3382 - reprints@alm.com.

DEFEND TRADE SECRETS ACT

ONE-PAGE SUMMARY

Background –

Trade secrets, such as manufacturing processes, formulas and customer lists, are an essential intellectual property right. The trade secrets of U.S. publicly listed companies alone are worth approximately \$5 trillion. Despite their strategic economic importance, trade secrets are the only form of U.S. intellectual property for which the owner lacks access to federal court for misappropriation. This leaves U.S. companies without a key tool to prevent trade secret theft and recover for any losses.

Trade secrets can be stolen with a few keystrokes, and increasingly they are stolen at the direction of foreign governments or for the benefit of foreign competitors. Once a trade secret has been stolen and sold to a competitor or made public, it may be gone for good because trade secrets lose their legal protection if they cease to be secret. Trade secret theft costs U.S. businesses hundreds of billions of dollars each year. This puts U.S. jobs at risk and threatens incentives for continued investment in research and development.

The Economic Espionage Act of 1996 makes trade secret theft a crime, but the Department of Justice lacks the resources to prosecute many such cases. Unfortunately, while trade secret owners have a remedy under state laws, state courts are not well suited to working across state and national boundaries to facilitate discovery, serve defendants or witnesses, or prevent a party from leaving the country. The Defend Trade Secret Act addresses these problems by empowering companies to protect their own trade secrets in federal court, creating a more efficient remedy.

Defend Trade Secrets Act Key Points –

- **The Defend Trade Secrets Act harmonizes U.S. law.** Building off of the Economic Espionage Act, the bill creates a uniform standard for trade secret misappropriation. Companies can craft one set of nondisclosure policies secure in the knowledge that its trade secrets will be protected by federal law.
- **The Defend Trade Secrets Act provides for injunctions and damages,** including a narrow, but powerful, *ex parte* seizure authority when it is needed to prevent the disclosure or further dissemination of a stolen trade secret. The bill also authorizes appropriate final monetary and injunctive relief to account for the economic harm to American companies whose trade secrets are stolen, while also safeguarding the freedom of employees to move from one job to another.
- **The Defend Trade Secrets Act is consistent** with the remedies provided for other forms of intellectual property, such as patents, trademarks and copyrights, which are all covered by federal civil law.
- **The Defend Trade Secrets Act will not lead to more litigation.** Trade secrets cases are already permitted under state law, but inconsistency in state laws and unavailability of key equitable remedies reduces their effectiveness. By providing a single uniform cause of action in federal court, trade secret litigation will be more effective and efficient. Lastly, state law will continue to apply, and state courts will continue to have jurisdiction over state law claims.